


| | | |
|---|---|---------------------------------|
|  | STANDARD OPERATING GUIDELINE SAN JUAN ISLAND EMERGENCY MEDICAL SERVICES SAN JUAN COUNTY PUBLIC HOSPITAL DISTRICT NO.1 | |
| | Global HIPAA Guidelines and Procedures | SOG # 141-11 |
| | Approved: Chief Jim Cole | ISSUED August 1, 2011 |

GLOBAL HIPAA GUIDELINES

I. General Security of Electronic and Other Patient and Business Information

Purpose

San Juan Island EMS is committed to providing all aspects of our service and in conducting our business operations in compliance with all applicable laws and regulations. This policy set forth our commitment for compliance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the use and disclosure of Protected Health Information ("PHI") under the Privacy Regulations ("Privacy Rule") and the security of Electronic Protected Health Information ("e-PHI") under the Security Regulations (the "Security Rule").

This policy and our procedures as to the creation, use, disclosure, and security of PHI and e-PHI also applies to other essential patient information, billing and business information, and confidential information that is stored electronically or in any other manner, including paper or hard copy form.

Scope

This Policy addresses our general approach to compliance with the Security Rule. As a covered entity under the Security Rule, San Juan Island EMS is required to:

- (1) ensure the confidentiality, integrity and availability of all PHI and e-PHI San Juan Island EMS creates, receives, maintains or transmits;
- (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

(3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and

(4) ensure compliance with the Privacy and Security Rule by our staff.

Compliance with the Privacy and Security Rules will require San Juan Island EMS to implement:

- Administrative Safeguards--actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect PHI and e-PHI and to manage the conduct of our staff in relation to the protection of and authorized access to patient information.
- Physical Safeguards--physical measures, policies and procedures to protect our electronic information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
- Technical Safeguards--the technologies and the policies and procedures for its use that protect PHI and e-PHI and control access.

Procedure

Information Security Officer

San Juan Island EMS has designated a Privacy/Information Security Officer with overall responsibility for the development and implementation of policies that conform to the Privacy Rule ("Privacy Policies") and the Security Rule ("Security Policies"). The Information Security Officer is responsible for ensuring that San Juan Island EMS: (i) complies with the HIPAA Security Policies, (ii) develops and implements HIPAA security procedures ("Security Procedures") for each Security Policy, (iii) maintains the confidentiality of all e-PHI created or received by San Juan Island EMS (as well as other essential patient information, billing and business information, and confidential information that is stored electronically) from the date the information is created or received until it is destroyed, and (iv) trains all staff members of San Juan Island EMS at the appropriate level of HIPAA training as determined by the Information Security Officer and Privacy Officer.

Implementation of Security Measures

San Juan Island EMS will implement any security measure that allows it to reasonably and appropriately comply with a specific security standard in the Security Rule. In determining which security measures to implement, San Juan Island EMS will take into account its size, complexity and capabilities; technical

infrastructure; hardware and software security capabilities; the costs of the security measures; and the probability and criticality of potential risks to e-PHI.

San Juan Island EMS will determine what security measures *must* be implemented and will determine those measures that we have *discretion* to implement. The determination as to what security measures are required or discretionary will be reviewed by the Privacy/Information Security Officer to ensure compliance with the Security Rule.

Security Complaints

The Information Security Officer shall be responsible for facilitating a process of individuals (including staff members) to file a complaint regarding our Security Policies or the manner in which e-PHI and other confidential information is handled. The Information Security Officer is responsible for ensuring that the complaint and its disposition are appropriately documented and handled.

Mitigation, Sanctions and Non-Retaliation

San Juan Island EMS will ensure it mitigates damages that may occur as a result of any violation of the Security Rule or our Security Policies or specific Security Procedures.

Any staff members who violate the Security Rule or San Juan Island EMS policies with respect to e-PHI and other protected and confidential information will be disciplined accordingly. This may include verbal or written counseling, suspension, or even termination, depending upon the seriousness of the infraction.

San Juan Island EMS will not intimidate or retaliate against any person for exercising his or her rights under the Security Rule or for reporting any concern, issue or practice that the person believes in good faith to be in violation of the Security Rule or our Security Policies or specific Security Procedures.

San Juan Island EMS will not require any person to inappropriately waive any rights that person may have to file a complaint with the Department of Health and Human Services.

Security Policies and Procedures

The San Juan Island EMS Security Policies and Security Procedures are designed to ensure compliance with the Security Rule. These Security Policies and Security Procedures will be kept current and in compliance with any changes in the law or regulations. There will be periodic evaluation of our Security Policies and Procedures whenever there are significant changes in the law or regulations or at least on an annual basis when there are no such changes.

Responsibility of All Staff Members

San Juan Island EMS takes privacy issues very seriously, especially in light of the unique work that we do in EMS and medical transportation. We will only recruit, hire, or accept staff members who are sensitive to patient privacy and who demonstrate a commitment to the principles of protecting our patient information and our business and other confidential information.

Every member of the San Juan Island EMS staff is responsible for being aware of, and complying with, the Privacy Rule, the Security Rule, and our Privacy and Security Policies and Procedures. This is an essential requirement of all positions within the organization.

Supervision of Staff Members Who Work With e-PHI

All staff members who use, access or work with e-PHI shall be supervised by appropriate members of management in accordance with their level of e-PHI access. For instance, the use of e-PHI by staff members in the billing department will be supervised by the billing department manager or other appropriate member of management who oversees that function. The use of e-PHI by field providers will be supervised by the appropriate field/operations supervisory personnel and/or line officers as appropriate.

II. Information Security Risk Assessment and Analysis

San Juan Island EMS is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The foundation of compliance with the Security Rule is the completion of a "Risk Assessment" to identify existing and potential flaws in the security of our electronic information system, and the related computer systems that are part of it. This policy describes our general approach to Risk Assessment under the Security Rule.

Scope

This policy applies to all San Juan Island EMS staff members who create, receive or use PHI and e-PHI, and any other confidential patient or business information. It is intended to cover all information system hardware, software and operational procedures.

Procedure

The Privacy/Information Security Officer will develop and implement a documented risk assessment procedure. This procedure will form the basis for identifying all critical information system assets and resources, and to evaluate the potential security problems that may occur.

San Juan Island EMS management personnel will undertake a risk analysis process that includes the following:

- Determine and identify the sources of e-PHI within the organization and the manner in which it is stored and transmitted.
- Determine the type of and degree of threats or potential threats to the information system where e-PHI is stored and utilized.
- Identify all potential vulnerabilities to the information system.
- Evaluate the likelihood of risk occurrence (all potential and actual threats to e-PHI will be identified and logged).
- Determine the impact that risks and vulnerabilities to those risks may have on the information system.
- Determine changes that need to be made to minimize the impact of all risks and vulnerabilities to the information system and the cost of those changes.
- Provide recommendations to improve and control the security of the information system.

The Risk Assessment will be evaluated against the cost of implementation of each of the recommendations.

Implementation specifications under the Security Rule that are “required” must be implemented and documented that they were in fact implemented, including how the specification was implemented.

Implementation specifications under the Security Rule that are “addressable” will be implemented as follows. The assessment of the addressable standards will be periodically reviewed and assessed:

- If the implementation specification is reasonable and appropriate, San Juan Island EMS will implement it.

- If the implementation specification is determined to be inappropriate and/or unreasonable, but the security standard cannot be met without implementation of an additional security safeguard, San Juan Island EMS may implement an alternative measure that achieves the addressable specification.
- If San Juan Island EMS meets the standard through alternative measures, the decision not to implement the specification will be documented, including the reason for the decision, the rationale, and a description of the alternative safeguard that was implemented.

III. Commitment to Protecting the Privacy and Security of Patient Information

Purpose

San Juan Island EMS is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

A cornerstone of compliance with these regulations is to conduct both a “Gap Analysis” to review and determine where compliance efforts must be focused under the Privacy Rule, and a “Risk Assessment” to identify threats and potential threats to the security of our electronic information system and computer network. This includes ensuring the confidentiality, availability and integrity of protected health information (PHI) stored in non-electronic formats such as paper, and electronic protected health information (e-PHI), the health information stored in our computer system.

This policy provides an overview of our compliance activities in these two important areas of privacy protection for our patients, and identifies our commitment to following industry “best practices” in all areas of compliance with the privacy regulations.

Scope

This policy applies to all San Juan Island EMS staff members who create, receive or use PHI and e-PHI, and any other confidential patient or business information.

Procedure

Privacy “Gap” Analysis

- The Privacy Officer will perform a Privacy Gap Analysis utilizing the Privacy Gap Analysis Tool
- The Privacy Officer will report the results of the Privacy Gap Analysis to management
- Management will implement the appropriate forms, policies, procedures, training, etc. necessary to implement the required privacy measures.

Security Risk Assessment

- The Information Security Officer will perform a Security Risk Assessment utilizing the Security Risk Assessment Tool.
- The Information Security Officer will report the results of the Security Risk Assessment to management.
- Management will implement the appropriate forms, policies, procedures, training, etc. necessary to implement the required security measures.

IV. Patient Access, Amendment And Restriction On Use of PHI

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 San Juan Island EMS 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.

Scope

This policy applies to all San Juan Island EMS staff members who handle requests from patients for access, amendment and requests for restriction on the use of PHI.

Procedure

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 San Juan Island EMS.

Patient Access

1. Upon presentation to the business office, the patient or appropriate representative will complete a Request for Access Form.
2. The District staff member must verify the patient's identity, and if the requestor is not the patient, the name of the individual and reason that the request is being made by this individual. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose.
3. The completed form will be presented to the Privacy Officer for action.
4. The Privacy Officer will act upon the request within 30 days, preferably sooner. Generally, the District 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 District 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 District could not respond within the time frame, and in that case the District may extend the response time by an additional 30 days.
6. Upon approval of access, the patient will have the right to access the PHI contained in the DRS outlined below and may make a copy of the PHI contained in the DRS upon verbal or written request.
7. The 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 District for review.

9. The following reasons to deny access to PHI are not subject to review and are final and may not be appealed by the patient:
 - a. If the information the patient requested was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;
 - b. If the information the patient requested was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

10. The following reasons to deny access to PHI are subject to review and the patient may appeal the denial:
 - a. If a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
 - b. If the protected health information makes reference to another person (other than a health care provider) and a licensed health professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that person;
 - c. If the request for access is made by a requestor as a personal representative of the individual about whom the requestor is requesting the information, and a licensed health professional has determined, in the exercise of professional judgment, that access by you is reasonably likely to cause harm to the individual or another person.
 - d. If the denial of the request for access to PHI is for reasons a, b, or c, then the patient may request a review of the denial of access by sending a written request to the Privacy Officer.
 - e. The District will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny the patient access. The District 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 District 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 District'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 District 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 District may charge a reasonable fee for the cost of reproduction.
13. Whenever a patient or requestor accesses a DRS, a note should be maintained in a log book indicating the time and date of the request, the date access was provided, what specific records were provided for review, and what copies were left with the patient or requestor.
14. Following a request for access to PHI, a patient or requestor may request an amendment to his or her PHI, and request restriction on its use in some circumstances.

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 District must act upon a Request for Amendment within 60 days of the request. If the District 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 the District may notify the persons with which the amendments need to be shared. The District must provide the amended information to those individuals identified 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.
20. The patient must identify individuals who may need the amended PHI and sign the statement in the Request for Amendment form giving the District permission to provide them with the updated PHI.
21. The District 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 District to the designated record set.

Denial of Requests for Amendment

22. The District may deny a request to amend PHI for the following reasons: 1) If the District 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 District 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 District's option, a summary of the disagreement will be appended, along with the rebuttal statement of the District.
25. If the District 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 District 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 District 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 DISTRICT FORM. ALL REQUESTS WILL BE REVIEWED AND DENIED OR APPROVED BY THE PRIVACY OFFICER.
29. If the District 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 services, and the restricted PHI is needed to provide the emergency services, the District may use the restricted PHI or may disclose such PHI to another health care provider to provide treatment to the individual.
30. The agreement to restrict PHI will be documented to ensure that the restriction is followed.
31. A restriction may be terminated if the individual agrees to or requests the termination. Oral agreements to terminate restrictions must be documented. A current restriction may also be terminated by the District, as long as the District notifies the patient that PHI created or received after the restriction is removed is no longer restricted. PHI that was restricted prior to the District voiding the restriction must continue to be treated as restricted PHI.

V. Privacy and Information Security Training

Purpose

To ensure that all members of San Juan Island EMS Staff -- 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 District's policies and procedures regarding Protected Health Information (PHI) and the security of e-PHI.

Scope

This policy applies to all San Juan Island EMS staff members. This includes those who have access to PHI or e-PHI, as well as those who do not ordinarily have access or a need to access to it.

Procedure

1. All current staff will be required to undergo privacy and security training in accordance with the HIPAA Privacy Rule and the HIPAA Security Rule. (Security training must occur before April 20, 2011.)
2. All new staff members will be required to undergo privacy training in accordance with the HIPAA Privacy and Security Rules within a reasonable time upon association with the organization, as scheduled by the Privacy/Information Security Officer.
3. All staff members will be required to undergo privacy training in accordance with the HIPAA Privacy and Security Rules within a reasonable time after there is a material change to the District's policies and procedures on privacy practices and the security of patient information.
4. The Privacy and Security Training will be conducted by the Privacy/Information Security Officer or his or her designee.
5. All attendees will receive copies of the District's policies and procedures regarding privacy and security of e-PHI.
6. All attendees must personally complete the training and verify completion and agreement to adhere to the District's policies and procedures on privacy and security practices.
7. Training will be conducted in the following manner: All staff and volunteers will receive annual Privacy and Security Training. Methods used include video tapes, classroom and computer generated instruction and testing of comprehension material.
8. Topics of the training will include a complete review of the District's privacy and security policies and procedures and will include other

information concerning the HIPAA Privacy and Security Rules, such as, but not limited to, the following topic areas:

- a. Overview of the federal and state laws concerning patient privacy including the Privacy and Security Regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- b. Description of protected health information (PHI) and electronic protected health information (e-PHI)
- c. Patient rights under the HIPAA Privacy Rule
- d. Staff member responsibilities under the Privacy and Security Rules
- e. Role of the Privacy/Information Security 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 and security policies
- h. Use of the District's specific privacy and security forms

VI. Assignment of Responsibilities: The Privacy and Information Security Officers

Purpose

San Juan Island EMS is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Scope

This policy applies to all San Juan Island EMS staff members who create, receive or use PHI and e-PHI, and any other confidential patient or business information. It outlines the role of the Privacy Officer and Information Security Officer and how those responsibilities relate to all San Juan Island EMS staff members.

Procedure

Both privacy and security compliance under HIPAA are very important responsibilities. San Juan Island EMS will assign the responsibility of Privacy Officer and Information Security Officer to a staff member knowledgeable about the Privacy and Security Rules, and who will be able to devote the time and energy to the important responsibilities that come with this assignment.

The Privacy Officer and Information Security Officer are high level positions in the organization and as such, the persons assigned to these responsibilities will have access to the highest levels of management to review and discuss policies and procedures, as well as compliance issues and concerns related to the HIPAA Privacy and Security Regulations.

The Privacy Officer and the Information Security Officer may be the same person, since the privacy-related responsibilities between the Privacy Rule and the Security Rule are similar in many respects. San Juan Island EMS may also break out the privacy and security compliance responsibilities into two separate positions, depending on workload and organizational need. The Privacy and Information Security Officers may delegate appropriate duties to other responsible staff members.

The following is an overview of the compliance responsibilities of both functions:

Privacy Officer Responsibilities

The Privacy Officer oversees all activities related to the development, implementation, and maintenance of San Juan Island EMS'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) and the Privacy Regulations under that law.

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.

- Develops policies and procedures on staff training related to the privacy of patient health information and protected health information.
- Defines levels of staff access to PHI and minimum necessary requirement for staff based on the required job responsibilities.

- Oversees, directs, delivers, and ensures the delivery of initial and ongoing privacy training and orientation to all staff members, employees, volunteers, students and trainees.
- Serves as the contact person for the dissemination of PHI to other health care providers.
- Serves as the contact person for patient complaints and requests.
- Processes patient requests for access to and amendment of health information and consent forms.
- Processes all patient accounting requests.
- Ensures the capture and storage of patient PHI for the minimum period required by law.
- Ensures ambulance service compliance with all applicable Privacy Rule requirements and works with legal counsel and other managers to ensure the District maintains appropriate privacy and confidentiality notices and forms and materials.
- Cooperates with the state and federal government agencies charged with compliance reviews, audits and investigations related to the privacy of patient information.

Information Security Officer Responsibilities

The Information Security Officer oversees all activities related to the development, implementation, and maintenance of San Juan Island EMS's policies and procedures covering the security of electronic patient health information (e-PHI). This person serves as the key compliance officer for all federal and state laws that apply to the security of patient information, including the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Security Regulations under that law.

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.

- Ensures that the necessary and appropriate HIPAA related policies are developed and implemented to ensure the security and integrity of all e-PHI within our District and as provided to our business associates.

- Ensures that the necessary infrastructure of personnel, procedures and systems is in place to develop and implement the necessary HIPAA- related policies with respect to the security of e-PHI.
- Ensures that the necessary infrastructure of personnel, procedures and systems is in place to assess, analyze, monitor, and review San Juan Island EMS's compliance with all HIPAA-related security policies.
- Develops policies on the security of health care information, including computer and password security and patient data integrity.
- Ensures that the necessary infrastructure of personnel, procedures and systems is in place to provide a mechanism for reporting security incidents and HIPAA security violations.
- Acts as a spokesperson and single point of contact for San Juan Island EMS in all issues related to HIPAA security.
- Periodically reviews all security policies to ensure that they maintain their viability and effectiveness.
- Develops and conducts educational programs for San Juan Island EMS staff to help ensure their compliance with all e-PHI policies and procedures.
- Cooperates with the state and federal government agencies charged with compliance reviews, audits and investigations related to the security of patient information.

VII. Contracting with Business Associates

Purpose

San Juan Island EMS is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

An important aspect of protecting this information is to ensure that those persons and entities we trust to use patient information on our behalf protect it as we would. This policy describes our approach to entering into agreements with persons and organizations outside of San Juan Island EMS, who perform services on our behalf. They must be required, under penalty of termination of the agreement, to abide by all privacy and security regulations.

Scope

This policy applies to all San Juan Island EMS staff members who are responsible for entering into agreements with outside vendors or persons.

Procedure

1. San Juan Island EMS will identify persons and organizations that perform services on our behalf and who in any manner use or store confidential and protected health information about our patients.
2. All such persons are called “business associates” (BAs) of San Juan Island EMS, and they must agree to our privacy and security of information procedures and requirements if they wish to do business with us.
3. All managers are required to identify business associates in their respective areas, and report them to the Privacy Officer.
4. The Privacy Officer will maintain a current list of business associates.
5. All contracts and agreements between San Juan Island EMS and any contractor that may come into contact with PHI that we create, use or store in any manner to ensure that business associate language and protections are included in the contract terms.
6. Managers must ensure that in any agreements with a business associate where there is a BA agreement separate from the main agreement that the main agreement specifically refers to the BA agreement.
7. All managers must ensure that, in any relationship with a vendor that is identified as a business associate (even those where there is no written contract), a written business associate agreement is signed.
8. No disclosures of PHI or e-PHI will be made by any staff member until it is verified that there is a current BA agreement on file.
9. The Privacy Officer will be responsible for maintaining BA agreements on file for periodic review and inspection.

VIII. Evaluating and Updating HIPAA Policies, Procedures and Training

Purpose

San Juan Island EMS is responsible for ensuring the privacy and security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

San Juan Island EMS has adopted this policy to ensure that its Privacy and Security Policies, Procedures and Training are up to date and effective in safeguarding the confidentiality, integrity and availability of PHI and e-PHI created, received, maintained and transmitted by SAN JUAN ISLAND EMS. It is the goal of San Juan Island EMS to adjust our policies and procedures accordingly based on periodic reviews and evaluations of our privacy protection systems.

Scope

This policy applies to all San Juan Island EMS staff members who have access to or use PHI or e-PHI and the managers who are responsible for providing the updates in privacy and security practices to staff members. The Privacy/Information Security Officer will have overall responsibility for monitoring all new developments in patient privacy and security of patient information and will recommend updates to the compliance program as necessary

Procedure

Maintaining Knowledge

1. The Privacy/Information Security Officer will strive to keep current with all changes in the law and regulations that address the privacy and security of patient information.
2. The Privacy/Information Security Officer will subscribe to professional journals and newsletters on the subject of privacy protection, and will sign up for appropriate list-serves to obtain current information.
3. The Privacy/Information Security Officer will monitor Internet sites periodically for new information on compliance issues related to patient privacy.
4. The Privacy/Information Security Officer will attend seminars and conferences on privacy protection as needed and as the budget allows.

5. The Privacy/Information Security Officer will consult with legal counsel as necessary to learn of new legal developments that could affect San Juan Island EMS with respect to privacy issues.

Evaluation of Policies and Procedures

1. On at least an annual basis, the Privacy/Information Security Officer will convene a committee of managers and staff members to identify and review all existing policies and procedures for compliance with current law and regulations regarding privacy.
2. Any member of the review committee or any other staff member may suggest changes to our Privacy and Security Policies or Procedures by submitting the suggestion to the Privacy/Information Security Officer for consideration.
2. The annual policy and procedure review will include an identification of all changes that need to be made to our policies, based on the experience of staff and management and changes in the regulatory environment during the prior year.
3. Any critical changes in the law or regulations that require a change in our privacy practices will be addressed immediately and incorporated into our privacy compliance program.
4. All complaints and concerns regarding the safeguarding of patient information will be evaluated by the Privacy/Information Security Officer to determine if policy or procedure changes need to be implemented.
5. Unwritten procedures and practices will also be reviewed to ensure compliance with the Privacy and Security regulations.

Evaluating and Updating Training Programs

1. The Privacy/Information Security Officer will be the keeper of all HIPAA-related training materials and will update those materials and keep them current with recent changes in privacy practices as necessary.
2. Additional in-District training will be scheduled as necessary to ensure that all staff members are kept up to date.
3. An updated privacy and security training program will be provided to the staff on an annual basis.
4. New staff members will be provided with updated privacy and security training upon employment and as otherwise necessary.

Updating Password Assignments

1. The Privacy/Information Security Officer will monitor the use of passwords to access the electronic information system.
2. On an annual basis, the Privacy/Information Security Officer will update the password assignment policy and recommend any necessary changes.
3. All San Juan Island EMS staff members will keep, use, protect and change their access passwords in accordance with the procedures communicated by the Privacy/Information Security Officer.
4. All staff members must adhere strictly to the password procedures established by the District.

Annual Security Assessment

1. The Privacy/Information Security Officer will develop a process for completing an annual “walk through” of all areas where e-PHI is used, stored, or transmitted.
2. The walk through will be used to identify strengths and weaknesses in our current security compliance program and to make recommended changes to update our process as needed.
3. Physical security changes will be implemented based on the results of this the annual walk through, and through information collected from other sources, such as staff members, other managers, business associates, and patients.

IX. Workforce Sanction Policy for Violation of Privacy and Security Policies and Procedures

Purpose

San Juan Island EMS is responsible for ensuring the privacy and security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

An important aspect of protecting this information is to make it clear to all staff members that San Juan Island EMSs takes privacy and security issues very seriously. Any breach of our privacy and security policies are very serious. Not only does the

law require that we appropriately sanction staff members for privacy violations, our patients and the public expect us to do just that.

This policy describes our approach to staff member sanctions when there is a violation of our privacy and security policies.

Scope

This policy applies to all San Juan Island EMS staff members who have any degree of access to patient information, including those staff members who may learn of patient information indirectly, and even if use of this information is not part of the staff member's responsibilities with SAN JUAN ISLAND EMS.

Any sanctions under this policy or any other policy will not apply to staff members who 1) file a complaint with the federal government about potential privacy violations, 2) testify, assist, or participate in an investigation or compliance review proceeding or official government proceeding investigating privacy issues, and 3) oppose any actions by San Juan Island EMS that are unlawful under the HIPAA Privacy Rule or the HIPAA Security Rule, when that opposition is made with the good faith belief that SAN JUAN ISLAND EMS was violating privacy or security regulations (as long as any opposition or filing of a complaint did not result in improper disclosure of PHI or e-PHI).

Procedure

1. San Juan Island EMS will implement sanctions that are to be used when any staff member fails to comply with or violates our privacy policies and procedures.
2. Sanctions will be administered in a progressive manner wherever possible. San Juan Island EMS will administer sanctions to the degree necessary to correct improper behavior or to protect patient privacy.

(EXAMPLE: A first time violation where an employee revealed PHI to another staff member without any need to know may receive a verbal counseling or written warning, but if a first violation resulted in revealing PHI to someone who was not a staff member or business associate, a suspension may be warranted.)

3. Progressive sanctions will include the following:
 - a. Remedial training and education
 - b. Informal verbal counseling

- c. Formal verbal counseling with written documentation of the counseling
 - d. Written warning
 - e. Suspension
 - f. Termination or expulsion from San Juan Island EMS
4. Staff members have an affirmative duty to report to management or the Privacy Officer or Information Security Officer any suspected violation of our privacy/security policies and procedures.
 5. Staff members shall be educated about this policy and the serious nature of violating our privacy/security policies. Staff members will be made aware of the potential sanctions that may occur, and will be made aware of any changes to this sanction policy.
 6. A record of individual staff member sanctions will be kept in the respective staff member's file. Adherence to our privacy/security policies will be considered as part of the staff member's performance evaluation.
 7. In the event of a suspected or reported violation of our privacy/security policies, the Privacy/Information Security Officer will initiate an objective and comprehensive investigation that will include:
 - a. Interviews of potential witnesses
 - b. Interviews of the alleged violator
 - c. Preparation of an investigative report
 - d. Presentation of the report to management with recommendations for sanctions (if any) or changes in our policies or practices
 8. At all times, whenever there is a suspected violation of our policies or other breach of privacy, the Privacy/Information Security Officer will recommend immediate action to be taken to mitigate the violation and its impact on San Juan Island EMS.

X. Levels of Access, "Minimum Necessary Standard" and Limiting Disclosure and Use of PHI and e-PHI

Purpose

San Juan Island EMS, in accordance with the Privacy and Security Rule, will only disclose the minimum amount of patient information that is needed to accomplish the purpose for which the disclosure is made. This does not in any way limit the amount of patient information that may be exchanged between staff

members or between staff members and other health care providers during the course of treatment and transport of the patients we serve.

Security of PHI and e-PHI is everyone's responsibility. This policy outlines levels of access to Protected Health Information (PHI) and electronic protected health information (e-PHI) of various staff members of San Juan Island EMS and provides our policy and general procedures on limiting access, disclosure, and use of PHI.

Policy

San Juan Island EMS retains strict requirements on the security, access, disclosure and use of PHI and e-PHI. Access, disclosure and use of PHI and e-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 patient information to complete necessary responsibilities for SAN JUAN ISLAND EMS.

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

Procedure

Role Based Access

Access to PHI and e-PHI will be limited to those who need access to carry out their duties. The following describes the specific categories or types of PHI and e-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 and e-PHI to Be Accessed | Conditions of Access to PHI and e-PHI |
|-----------|--|--|
| EMT | Intake forms from dispatch, patient care reports | May access only as part of completion of a patient event and post-event activities and only while actually on duty |
| Paramedic | Intake forms from dispatch, patient care reports | May access only as part of completion of a patient event and post-event activities and only while actually on duty |

| | | |
|----------------------|--|--|
| 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 duties to complete patient billing and follow up and only during actual work shift |
| Field 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 |
| Administrators | Intake forms from dispatch, patient care reports and billing information | May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel |

Access to PHI and e-PHI is limited to the above-identified persons only, and to the identified patient information only, based on the District'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.

This policy does not prevent the release of any patient information among staff members or among staff members and other health care providers necessary to carry out proper treatment and transport of the patient.

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 or e-PHI to patients

who are the subject of the information. In addition, disclosures authorized by the patient are exempt from the minimum necessary requirements unless the authorization to disclose PHI or e-PHI is requested by the District.

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

For example, if we have a patient's authorization to disclose PHI or e-PHI to Medicare, Medicaid or another health insurance plan for claim determination purposes, the District is permitted to disclose the information requested without making any minimum necessary determination.

District Requests for PHI and e-PHI

If the District needs to request PHI or e-PHI from another health care provider on a routine or recurring basis, we must limit our requests to only the reasonably necessary information needed for the intended purpose, as described below. For requests not covered below, you must make this determination individually for each request and you should consult your supervisor for guidance. For example, if the request is non-recurring or non-routine, like making a request for documents via a subpoena, we must review make sure our request covers only the minimum necessary amount of information needed to accomplish the purpose of the request.

| Holder of PHI or e-PHI | Purpose of Request | Information Reasonably Necessary to Accomplish Purpose |
|----------------------------|--|--|
| Skilled Nursing Facilities | To have adequate patient records to determine medical necessity and to properly bill | 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 and to properly bill | Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments |
| | | |

| | | |
|--|--|----------------------|
| Mutual Aid Ambulance or Paramedic Districts | To have adequate patient records to conduct joint billing operations for patients mutually treated/transported by the District | Patient care reports |
|--|--|----------------------|

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

Incidental Disclosures

The District understands that there will be times when there are incidental disclosures about PHI or e-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 members 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.

But 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 services provided to them or to have billing questions answered, make sure that there are no other persons in the waiting area, or if so, bring the patient into a screened area before engaging in discussion.

Garage Areas: Staff members should be sensitive to the fact that members of the public and other agencies may be present in the garage and other easily

accessible areas. Conversations about patients and their health care should not take place in areas where those without a need to know are present.

Other Areas: Staff members should only discuss patient care information with those who are involved in the care of the patient, regardless of your physical location. You should be sensitive to your level of voice and to the fact that others may be in the area when you are speaking. This approach is not meant to impede anyone's ability to speak with other health care providers freely when engaged in the care of the patient. When it comes to treatment of the patient, you should be free to discuss all aspects of the patient's medical condition, treatment provided, and any of their health information you may have in your possession with others involved in the care of the patient.

Physical Security

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

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

Computers and Entry Devices: Computer access terminals and other remote entry devices such as PDAs and laptops should be kept secure. Access to any computer device should be by password only. Staff members should be sensitive to who may be in viewing range of the monitor screen and take simple steps to shield viewing of the screen by unauthorized persons. All remote devices such as laptops and PDAs should remain in the physical possession of the individually to whom it is assigned at all times.

XI. Policy on Designated Record Sets

Purpose

To ensure that San Juan Island EMS 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 Designated Record Sets (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 District to make decisions about the patient.

Scope

This policy applies to all San Juan Island EMS staff members responsible for the designation of PHI into designated record sets. All staff members should be familiar with the information from the medical records that may be accessible to our patients.

Procedure

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.

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 should 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 District as part of treatment and payment purposes related to the patient.

XII. News Media Interaction Policy

Purpose

To provide consistent guidelines for personnel of San Juan Island EMS on what patient information, commonly referred to as protected health information ("PHI") may be permitted to disclose to the news media (i.e. newspaper, television).

This policy is necessary as federal law protects a patient's general right to privacy under the Privacy Regulations of the Health Insurance Portability and Accountability Act (HIPAA). State law protections from invasion of privacy may also apply.

As a general rule, since SAN JUAN ISLAND EMS is covered by HIPAA, we may not release PHI to anyone, absent a patient's written authorization, except for purposes of patient treatment, billing or other health care operations related to SAN JUAN ISLAND EMS. SAN JUAN ISLAND EMS may release certain information as long as the information is "de-identified," meaning that the person who receives the information would not likely be able to ascertain the identity of the patient with the information we provide.

We must balance providing the public with information about the services we provide against the individual rights of the patient to keep their medical information confidential. We fully respect the right of the public to know about our activities as we are a public agency subject to public scrutiny. But we can provide information to the public only to the extent that the law allows us.

We will at all times treat members of the media in a professional manner when a request for information is made.

Scope

This policy applies to all San Juan Island EMS staff members who come in contact with or are contacted by members of the various media.

Procedure

All requests for information from the news media shall be directed to the Public Information Officer. Staff members are not permitted to release information to the news media, including patient records or reports at any time except as authorized by a supervisor.

SAN JUAN ISLAND EMS maintains the highest standards of patient confidentiality. It is impossible, however, to accomplish this standard without the compliance of our staff. To ensure that there are no inappropriate disclosures or uses of a patient's PHI, only the following information may be disclosed by SAN JUAN ISLAND EMS to members of the media as follows:

Name of hospital. You may provide the name of the hospital to which patients have been transported. (Acceptable Example: The media calls about "the accident at Third and Main earlier this afternoon." You may inform the media "a patient was transported from the accident scene to Island Hospital."). **THE NAME OF THE PATIENT SHOULD NOT BE RELEASED TO THE MEDIA.** It is not appropriate for us to confirm or deny the identity of a patient. Requests for patient identity should be directed to a law enforcement agency or to the hospital. Law enforcement agencies are not subject to the strict requirements of protecting patient information as we are under HIPAA.

Number of patients. You may provide the total number of patients involved in an accident or transported to a facility. You may not indicate specifics about the vehicle a patient was driving or which patient went to a particular facility. (Acceptable Example: You may inform the media that "four patients were transported from the fire at the SAN JUAN ISLAND Chemical Factory. Two were taken to County General and two were taken to the Regional Medical Center.")

Age & Gender. You may provide the age of a patient and the gender of the patient, unless it could reasonably be used to identify the patient. (Acceptable Example: You may inform the media "a 39 y/o male was transported from the accident on the Interstate." You would not want to disclose to the media "a 39 y/o male was transported from 124 Main St.")

Designation of crew members. The designation of crew members as paramedics or EMTs is not protected health information. You may state, for example, that one paramedic and two EMTs were involved in caring for the patients involved in a motor vehicle accident. (You could identify the names of the personnel who responded, but some services prefer not to release this information). You are not permitted to describe the specific type of care rendered to patients at the scene or on the way to the hospital. Nor may you speculate on what injuries a patient may or may not have sustained. (Acceptable Example: SAN JUAN ISLAND EMS

personnel on the scene of the incident included two paramedics and a supervisor and advanced life support was administered.”)

Type of Transport. You may indicate that a particular call was an emergency and that transportation was facilitated by ambulance or helicopter. Do not speculate on the patient’s condition even if you are sure of that condition. For example, do not disclose to a member of the media that a patient was critical or stable unless you are comfortable in knowing this to be their general condition. (Acceptable Example: “Of the 3 patients on the scene of the incident, one was transported by helicopter to the Seattle Trauma Center and two were transported as non-emergency patients to the local hospital emergency department.”)

Non-PHI. Information that is not classified as PHI may be released to the media consistent with District policy and state law. For instance, information about a fire response or a standby that did not involve patient care may be released to the media, as may general information about an event. (Acceptable Example: “We treated 45 patients during the two-day festival, and 6 were transported to local hospitals for various heat-related complaints”).

Disclosures Authorized by the Patient. In the event that the patient or the patient’s legally responsible decision maker signs a HIPAA authorization form, disclosures of information, including PHI, may be made so long as they are done in accordance with the express terms of the written authorization. Authorization forms for this purpose must be HIPAA-compliant and must be approved by the Privacy Officer.

If at any time you are unclear about whether information may be disclosed to the media, always err on the side of caution and do not disclose the questionable item of information. Again, all requests for patient information should be directed to the Public Information Officer.

XIII. Release of Protected Health Information to Law Enforcement

Purpose

To provide consistent guidelines for personnel of San Juan Island EMS on when they may be permitted to disclose patient information to law enforcement. Under the federal privacy regulations, individually identifiable information about a patient’s medical situation is often protected from disclosure to others unless the patient authorizes that disclosure or any of the following exceptions are satisfied.

Scope

This policy applies to all San Juan Island EMS staff who may come in contact with law enforcement. This would include field personnel who may encounter law enforcement officials at the scene of an incident, as well as office staff who may receive official requests for information from law enforcement personnel.

Procedure

Protected health information, or PHI, is defined as individually identifiable health information, created or received by us, that relates to the past, present, or future physical or mental health of a patient, the provision of health care to the patient, or payment for the provision of health care to the patient.

PHI can be in any form including paper, electronic (e-PHI), or verbal. Typical examples of sources where PHI may be contained include PCRs, billing forms, and verbal information about a patient exchanged with others.

There are six (6) specific situations where some or all of a patient's protected health information (PHI) may be disclosed to law enforcement personnel. These situations fall into three (3) general categories:

- Disclosures required by law;
- Disclosures permitted by law; and
- Optional disclosures.

Procedure – Disclosures Required by Law

You are required by law to give a patient's PHI to law enforcement regardless of the patient's consent when law enforcement personnel present you with:

- A subpoena, summons, or warrant (“SSW”)
- An administrative request/investigative demand (see #3)
- A request for information pertaining to a limited number of injuries that you must disclose by law (see # 4)

Subpoena, Summons or Warrant. Confirm that the paper you receive is, in fact, a subpoena, summons or warrant and that it specifically identifies the PHI you are required to disclose.

A subpoena, summons or warrant is issued by a Court, judicial officer or grand jury. Be sure that the SSW has one of these designations as the issuer.

Patient care reports (PCRs). You may or may not be able to just turn over a copy of your PCR to law enforcement. If the SSW is valid, provide ONLY the PHI requested. You are legally required to disclose ONLY that information that is contained in the four corners of the paper you are given by law enforcement. You are not to disclose any other information not specifically requested.

If the SSW requests the entire PCR, or utilizes language such as “any and all records” pertaining to the patient, you must provide the entire PCR in response.

Do NOT disclose information based on a verbal request from law enforcement (see *Permitted Disclosures and Optional Disclosures for exceptions*).

Keep a copy of the SSW.

Please note: This section addresses SSWs issued by a judicial officer or a grand jury and served by law enforcement, *not* served by private litigants.

Administrative Request/Investigative Demand. An administrative request/investigative demand is a request for PHI by a federal/state/local government agency authorized to make such requests.

If you receive an administrative request/investigative demand, you may ONLY give out a patient’s PHI as long as the information requested is:

- Relevant and material to law enforcement’s inquiry,
- Specific and limited in scope to the inquiry, and
- Information (other than PHI) could not be used.

You should obtain assurances of the above three items from the agency making the investigative demand.

Burns, Firearm Injuries, Animal Bites, Abuse, Domestic Violence. EMS providers are legally obligated to report to law enforcement certain types of injuries like a gunshot wound, animal bites, burn or incidents of abuse (i.e., child abuse, elder abuse or domestic violence). State law governs these reporting requirements, and these types of disclosures of PHI are permitted where you are required to make such reports under state law. Contact your Supervisor for a list of those injuries that you must report under state law in the particular jurisdiction where you are employed.

Procedure – Permitted Disclosures

Here is a list of the approved situations where PHI may be disclosed, without the patient’s authorization, consent or permission, when law enforcement requests PHI for the purpose of:

- Identifying or locating a suspect, material witness or missing person;
- Victim of a crime; and
- Abuse, neglect and domestic violence.

Ask law enforcement the purpose of their request before disclosing PHI.

Identifying or locating a suspect, material witness, or missing person. If law enforcement indicates that they need the PHI to identify or locate a suspect, material witness, or missing person, you may disclose only the PHI listed below:

- Name
- Address
- Date of birth
- Place of birth
- Social Security Number
- Blood type
- Type of injury
- Date of treatment
- Time of treatment
- Description of distinguishing physical characteristics (i.e. weight, hair color, eye color, gender, facial hair, scars and tattoos)

Do NOT give law enforcement any PHI when the sole purpose of the request is to assist law enforcement with their investigation or to help build a case against a suspect unless an appropriate subpoena or warrant is presented. Law enforcement's request must conform to the procedures outlined in this policy.

Do NOT disclose for the purposes of identification or location any PHI related to the patient's:

- DNA or DNA analysis
- Dental records
- Typing, samples or analysis of body fluids or tissue

Victim of crime.

The law allows more latitude when disclosing information to law enforcement authorities when the information is about a victim of a crime. Victims of a crime may include motor accident victims because often a summary or misdemeanor offense is involved, such as when the accident is the result of the driver of another vehicle violating traffic laws. It is not our job to make the determination of whether the patient is an actual crime victim, and in many cases the determination that a patient is or may be a crime victim can be inferred from the circumstances and the presence of law enforcement at the scene.

First, the best approach is ask the patient (if the patient is conscious and alert) if it is acceptable to disclose the PHI to law enforcement. You may disclose PHI about a crime victim to law enforcement if the crime victim consents to the disclosure.

If your patient is temporarily unable to consent, ask law enforcement if they can wait until your patient is able to consent.

If law enforcement cannot wait until the patient is able to consent because to do so would compromise an immediate law enforcement need (i.e., to determine if a crime has occurred or to determine the location of victims who may need to be interviewed later), then you may disclose the patient's PHI.

Ask for and obtain law enforcement's assurance that the PHI you provide will not be used against the victim and that the information is needed immediately. While these assurances may be given verbally, document that you received them.

Abuse, neglect and domestic violence. You are permitted to disclose PHI about a patient whom you believe is a victim of abuse, neglect or domestic violence, where these disclosures are required by state law.

If you think your patient is a victim of abuse, neglect or domestic violence, you may disclose PHI to a government authority, including Social Services and law enforcement.

Ask the patient for his/her consent. If the individual agrees to the disclosure of PHI, you may give this information to law enforcement.

If the patient does not consent or is unable to consent, you may disclose PHI to law enforcement as required by State law if:

- You believe the disclosure is necessary to prevent serious harm to the patient or other potential victims, or
- The patient is unable to consent due to incapacity,
- Law enforcement assures you the PHI will not be used against the victim, and
- Law enforcement activities would be adversely affected without the PHI.

If you have disclosed PHI without the patient's consent or because the patient was unable to consent, the designated privacy official should contact the patient and alert them of the disclosure, unless you believe contacting the patient will only put the patient at greater risk.

Procedure – Optional Disclosures

Decedents. You may disclose PHI to law enforcement when you think your patient died as a result of a crime. Limit the PHI to basic facts about the victim and

the circumstances of the death. You may disclose PHI to a coroner regardless of the cause of death. [NOTE: Check your state law for specific requirements as to the coroner's authority and procedures the coroner may have to follow.]

Crime on Premises. You may disclose to law enforcement any PHI you in good faith believe constitutes evidence of a crime committed on your organization's premises. This includes the station house; headquarters; parking lot; the ambulance or engine, etc.

Reporting crime in an emergency. You may voluntarily offer PHI to law enforcement when you believe it is necessary to alert law enforcement to:

- The commission of a crime
- The nature of a crime
- The location of the crime
- The location of a crime victim
- The identity, description, and location of the perpetrator of a crime

General Procedures

On-scene communications must involve a common sense approach. Providing law enforcement with basic information about where you are taking a patient and the patient's general condition (critical, serious, minor, etc.) is normally permissible when the event is a motor vehicle accident or other situation where a crime may have occurred. Remember at all times that, if you see physical evidence of a potential crime (such as drug paraphernalia, strange white powder in a bag, etc.), this evidence normally should be reported and given to law enforcement officials if it is not proper to leave it in the location it was found.

Requests for patient information that do not occur at the scene of an incident, but come after the call is over, should be directed to your Supervisor or the Privacy Officer.

XIV. Access to the Information System and e-PHI

Purpose

San Juan Island EMS has established this policy to ensure that all staff members have appropriate access to e-PHI and PHI, and that his or her identity is properly verified before such access can be attempted. This policy also addresses procedures to prevent staff members and former staff members who should not have access to e-PHI and PHI from obtaining it, and for emergency access to the information system.

Scope

This policy applies to all San Juan Island EMS staff members who utilize the electronic information system. It covers key provisions concerning who may have access to e-PHI and PHI, the level of access they may have, protections to ensure proper user identification for access, and emergency access to e-PHI and PHI. This policy also addresses the steps to be followed to terminate access to e-PHI and PHI when a staff member's authorization to access has ended, such as when employment or membership is terminated.

Procedure

Person or Identify Authorization

To ensure that all individuals or entities that access e-PHI have been appropriately authenticated, the following procedures are established:

- Staff members seeking access to any network, system, or application that contains e-PHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.
- Staff members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and password, smart card, or other authentication information.
- Workforce members are not permitted to allow other persons or entities to use their Unique User ID and password, smart card, or other authentication information.
- A reasonable effort must be made to verify the authenticity of the receiving person or entity prior to transmitting e-PHI.

Security Unique User Identification

To uniquely identify and track one user or workforce member from all others, for the purpose of access control to all networks, systems, and applications that contain e-PHI, and the monitoring of access to the aforementioned networks, systems, and applications, the following procedures are established:

- Any staff member or authorized user that requires access to any network, system, or application that access, transmits, receives, or stores e-PHI, must be provided with a Unique User Identification Number.

- When requesting access to any network, system, or application that access, transmits, receives, or stores e-PHI, a staff member or authorized user must supply their previously assigned Unique User Identification in conjunction with a secure password.
- Staff members or authorized users must not allow anyone else to use their Unique User Identification or password.
- Staff members and authorized users must ensure that their User Identification is not documented, written, or otherwise exposed in an insecure manner.
- Staff members and authorized users must take all reasonable steps to ensure that their assigned User Identification is appropriately protected and only used for legitimate access to networks, systems, or applications.
- If a staff member or authorized user believes their User Identification has been comprised, they must report that security incident to the appropriate supervisor or the Information Security Officer.

Security Password Management

To ensure that passwords created and used by San Juan Island EMS to access any network, system, or application used to access, transmit, receive, or store e-PHI is properly safeguarded the following procedures are established:

- All staff members who access networks, systems, or applications used to access, transmit, receive, or store e-PHI must be supplied with a Unique User Identification and password to access e-PHI.
- All staff members must supply a password in conjunction with their Unique User Identification to gain access to any application or database system used to create, transmit, receive, or store e-PHI.
- A generic User Identification and password may be utilized for access to shared or common area workstations so long as the login provides no access to e-PHI. An additional Unique User Identification and password must be supplied to access applications and database systems containing e-PHI.
- All passwords used to gain access to any network, system, or application used to access, transmit, receive, or store e-PHI must be of sufficient complexity to ensure that it is not easily guessable.
- Managers of networks, systems, or applications used to access, transmit, receive, or store e-PHI, must ensure that passwords set by staff members meet the minimum level of complexity described in this policy.

- Managers of networks, systems, or applications used to access, transmit, receive, or store e-PHI are responsible for educating staff members about all password related policies and procedures, and any changes to those policies and procedures.
- Password “aging times” (i.e., the period of time a password may be used before it must be changed) may be implemented in a manner commensurate with the criticality and sensitivity of the e-PHI contained within each network, system, application or database.
- Staff members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:
 - Passwords are only to be used for legitimate access to networks, systems, or applications.
 - Passwords must not be disclosed to other staff members or individuals.
 - Staff members must not allow other staff members or individuals to use their password.
 - Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.

Security Password Structure

To ensure that all passwords used to control access to any network, system, application, media or file containing e-PHI are secure and not easily guessed, the following procedures are established:

- Passwords must be a minimum of eight characters in length.
- Passwords must incorporate three of the following characteristics:
 - Any lower case letters (a-z)
 - Any upper case letters (A-Z)
 - Any numbers (0-9)
 - Any punctuation or non-alphanumeric characters found on a standard ASCII keyboard (! @ # \$ % ^ & * () _ - + = { } [] : ; “ ‘ | \ / ? < > , . ~ `)

- Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.
- Passwords must not be words found in a dictionary.
- If a system does not support the minimum structure and complexity as detailed in this policy, one of the following procedures must be implemented:
 - The password assigned must be adequately complex to ensure that it is not easily guessed. If an alternative password structure must be implemented, the complexity of the chosen alternative must be defined and documented.
 - The current system must be upgraded to support the minimum HIPAA Security Password Structure.
 - All e-PHI must be removed and relocated to a system that supports the minimum HIPAA Security Password Structure.

Emergency Access to e-PHI and PHI

To ensure that access to critical e-PHI is maintained during an emergency situation, the following emergency access procedures are established: If a system contains e-PHI used to provide patient treatment, and the denial or strict access to that e-PHI could inhibit or negatively affect patient care, staff members responsible for electronic information systems must ensure that access to that system is made available to any caregiver in case of an emergency.

Termination of Access

To ensure that access to the information system and e-PHI is terminated when a staff no longer has authorization for access, the following procedure is established. This procedure also applies to terminations in employment or membership in the organization, retirement, resignation, leave of absence, or transfer to an area in the organization where the staff member is no longer authorized to access the information system.

- All supervisors will immediately notify the Privacy/Information Security Officer or and the information system administrator when a staff member has been separated from service with the District or when the person no longer is permitted access to the system.
- The staff member's access to the information system will immediately be disabled on the effective date of the separation or, if still on the staff, the effective date when authorization for access has ended.

- The staff member will be removed from all information system access lists.
- The staff member will be removed from all user accounts.
- The staff member will turn in all keys, tokens, or access cards that allow access to the information system.
- The “Staff Member Termination Checklist” (Form 34) will be completed by the supervisor the last day of the staff member’s authorized access.

XV. Contingency Planning Policy

Purpose

San Juan Island EMS is committed to providing all aspects of our service and in conducting our business operations in compliance with all applicable laws and regulations concerning the security and integrity of Protected Health Information (PHI), electronic protected health information (e-PHI) and other essential patient information, billing and business information, and confidential information that is stored electronically or by other means.

This policy describes the approach to ensuring that our response to an emergency or other occurrence that threatens or damages our computer, electronic, or other information systems is appropriate. This policy provides for the contingencies necessary to protect and preserve that information in accordance with the HIPAA Security Rule and other regulations.

Scope

This policy covers the procedures for protecting the integrity of PHI and other essential patient information, billing and business information, and confidential information in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains this information is affected, including:

- Applications and data criticality analysis
- Data backup
- Disaster recovery planning
- Emergency mode operation plan

Procedure

Applications and Data Criticality Analysis

Administration will assess the relative criticality of specific applications and data within the District for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.

The assessment of data and application criticality should be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

Data Backup Plan

Each functional area of the District (Operations, Billing, Administration) will establish and implement a Data Backup Plan that ensures that each area of the District will create and maintain retrievable exact copies of all PHI and other essential business information that is at a medium to high risk for destruction or disruption.

The Data Backup Plan must apply to all medium and high risk files, records, images, voice or video files that may contain PHI and other essential business information.

The Data Backup Plan must require that all media used for backing up PHI and other essential business information be stored in a physically secure environment such as a secure, off-site storage facility. Where backup media remains on site, it will be kept in a physically secure location, different from the location of the computer systems have been backed up.

If an off-site storage facility or backup service is used, a written contract or Business Associate Agreement must be used to ensure that the Business Associate will safeguard any PHI and other essential business information in an appropriate manner.

Data backup procedures and contingency plan shall be tested on a periodic basis to ensure that exact copies of PHI and other essential business information can be retrieved and made available whenever it is needed.

Each functional area of the District with medium and high risk PHI must submit its Data Backup Plan to the HIPAA Information Security Officer for approval.

Disaster Recovery Plan

To ensure that each functional area of the District can recover from the loss of

data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting information systems containing PHI or other essential business information, each area will establish and implement a Disaster Recovery Plan. The Plan must ensure that each area can restore or recover any loss of this information and the systems needed to make that information available in a timely manner.

The Disaster Recovery Plan will include procedures to restore PHI and other essential business information from data backups in the case of a disaster causing data loss.

The Disaster Recovery Plan will include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.

The Disaster Recovery Plan must be documented and easily available to the necessary personnel at all time, who should be trained to implement the Disaster Recovery Plan.

The disaster recovery procedures outlined in the Disaster Recovery Plan must be tested on a periodic basis to ensure that PHI and other essential business information and the systems needed to make e-PHI available can be fully restored or recovered.

Each functional area at a medium and high risk of compromise of PHI and other essential business information must submit its Disaster Recovery Plan to the HIPAA Information Security Officer for approval.

Emergency Mode Operation Plan

Each functional area of the District must establish and implement (as needed) procedures to enable continuation of administrative, patient care, and billing and business processes for protection of the security of PHI and other essential business information while operating in emergency mode. Emergency mode operation procedures outlined in the Emergency Mode Operation Plan must be tested periodically to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode. Each functional area at a medium and high risk of compromise of e-PHI must submit its Emergency Mode Operation Plan to the Information Security Officer for approval.

XVI. Disaster Management and Recovery of e-PHI

Purpose

San Juan Island EMS is responsible for ensuring that we have a process in place to ensure that we can recover from the catastrophic disruption of our information system and loss of any data or information, especially e-PHI, which may be stored on that system. This “Disaster Management” policy will be followed in an emergency situation such as or disaster such as fire, vandalism, terrorism, system failure, or natural disaster.

Scope

This policy applies to all San Juan Island EMS staff members who create, receive or use PHI and e-PHI, and any other confidential patient or business information. It is intended to cover all information system hardware, software and operational procedures.

Procedure

To ensure that San Juan Island EMS will be able to recover from a serious information system disruption, including situations that could lead to the loss of data in the event of an emergency or disaster (such as fire, vandalism, terrorism, system failure, or natural disaster) the following procedures are established:

- A disaster recovery plan will be established and implemented to restore or recover any loss of e-PHI and any loss or disruption to the systems required to make e-PHI available.
- The disaster recovery plan will be developed by staff members responsible for the maintenance of the security and integrity of the information system and will be reviewed and approved by the Privacy/Information Security Officer and senior management.
- The disaster recovery plan must include:
 - A data backup plan including the storage location of backup media.
 - Procedures to restore e-PHI from data backups in the case of an emergency or disaster that results in a loss of critical data.
 - Procedures to ensure the continuation of business critical functions and processes for the protection of e-PHI during emergency or disaster situations.

- Procedures to periodically test data backup and disaster recovery plans.
- Procedures to periodically perform an application and data criticality analysis establishing the specific applications and e-PHI that is necessary to maintain operation in an emergency mode.
- Procedures to log system outages, failures, and data loss to critical systems.
- Procedures to train the appropriate personnel to implement the disaster recovery plan.
- The disaster recovery plan must be documented and easily available to the necessary personnel at all times.

XVII. Physical Security of PHI and e-PHI

Purpose

San Juan Island EMS is obligated to establish physical safeguards to protect Electronic Protected Health Information (e-PHI) and other PHI, confidential information and business information. This policy establishes our procedure with respect to security measures to protect our electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion.

Scope

This policy applies to all San Juan Island EMS staff members. All of us must be on the lookout for any potential problems that could jeopardize the security of electronically stored information, especially e-PHI. This policy describes our general approach to facility security and the steps necessary to prevent a breach in the physical security system in place. It also describes our general procedures to limit physical access to electronic information systems and the buildings and rooms in which they are housed and our general procedures on disposal or reissuance of computer equipment.

Procedure

Facility Access Controls

Access to areas of our facility that contain our information system components will be granted only to those with a verifiable and approved business need to have access.

Access control will be established with physical hardware that prevents improper or inadvertent entry into a secure area. This hardware may include combination locks, swipe cards, smart cards and other devices on all doors housing our information system equipment.

San Juan Island EMS will retain facility security of any areas that we use within a building owned or under the control of another entity. In other words, any space in a building that we share with another entity will be maintained at the same level of security as if we owned the space. Specifically, we will protect that area from access by others in the buildings that are not part of San Juan Island EMS.

Disabling or circumventing any of the physical security protections is strictly prohibited. Any problems with physical security measures must be reported to your supervisor or the Information Security Officer.

Contingency Operations. San Juan Island EMS has established procedures that allow facility access in support of restoring lost data under our disaster recovery plan and emergency mode operations plan in the event of an emergency that could compromise our electronic information system.

Facility Security Plan. The Information Security Officer will be responsible for developing a facility security plan that protects our buildings from unauthorized physical access, tampering, and theft.

The plan will incorporate hardware to limit access to our buildings to only those persons with proper keys and/or access codes.

The Information Security Officer will maintain a current list of all staff members who have authorization to access our facilities.

Access Control and Validation Procedures. San Juan Island EMS has established procedures for controlling and validating a staff member's access to our facilities. Access to various areas of the facilities will be based on the role of the staff person and their need to access a particular area.

Access to locations that house our information system infrastructure will have the greatest limitations on access, and access to these critical areas will be reviewed frequently by management and the Privacy/Information Security Officer.

Maintenance Records. To help ensure that our physical security systems are in continuous operation, San Juan Island EMS has developed a maintenance program for all security devices, including locks, key pads, and other access devices.

Workstation Security and Use

A “workstation” is defined as any electronic computing device, such as a desktop computer, laptop computer, PDA, or any other device that performs similar functions, and electronic media stored in its immediate environment.

All workstations will be evaluated to consider the procedures that must be followed to ensure the security of patient and other critical information. The environment will be considered (such as if the workstation is in a large room with cubicles and no fixed walls, the back of an ambulance, a crew room or report writing room, etc.)

General principles of our workstation security program include the following:

- All workstations (including both fixed locations such as in our billing or business office, as well as mobile stations such as with portable workstations equipped for field use) are set with password protection so that the computer may not be accessed without the proper password.
- All workstations are set up to go “inactive” after a set time period so that if the staff member leaves the workstation and forgets to logout and shut down, access will not be permitted without the proper password.
- Procedures are established for each work area, depending on the nature of the work area to limit viewing of workstation device screens to only those operating the workstation wherever possible.
 - For example, in office areas, all screens will be pointed away from hallways and open areas. The screens will be pointed away from chairs or other locations in the office where unauthorized persons, such as patients, may sit within that office.
 - In field operations, ambulance personnel will need to follow procedures to ensure that the workstation device is not left in an open area, such as a countertop in the Emergency Department.

- Workstations will be set so that staff members may not inadvertently change or disable security settings, or access areas of the information system they are not authorized to access.
- Only those authorized to access and use the workstation will be permitted to use the workstation.
- No software may be downloaded or installed on the workstation in any manner without prior authorization. (This prohibition includes computer games, screen savers, and anti-virus or anti-spam programs)
- All staff members will “log off” the workstation whenever it is left unattended.
- All portable workstation devices will be physically secured wherever possible when not in use. Laptops will be locked with security cables and PDAs and other handheld devices will be locked in their cradles or in an appropriate storage compartment when not in use.
- Use of any dial up modems and remote access software to access the information system off site must be approved by the Privacy/Information Security Officer.
- Multiple network interface cards (NICs) that allow simultaneous network connections shall not be used in individual workstations unless approved by the Privacy/Information Security Officer.

Device and Media Controls

San Juan Island EMS carefully monitors and regulates the receipt and removal of hardware and electronic media that contain e-PHI, PHI and other patient and business information into and out of our stations and other facilities. These controls pertain to the movement, re-use, or disposal of hardware and media within San Juan Island EMS facilities.

As a general rule, simple deletion of files or folders is not sufficient to ensure removal of the file or data. This simply removes the directional “pointers” that allow a user to find the file or folder more readily. Deleted files are usually completely retrievable with special software and computer system expertise.

Disposal. San Juan Island EMS has in place procedures governing the disposal of hardware and electronic media:

- Sanitizing Hard Disk Drives. All hard disk drives that have been approved by the Privacy/Information Security Officer for removal and disposal (or taken out of active use) shall be sanitized so that all programs and data have been

removed from the drive. The District will follow industry best practices (such as the U.S. Department of Defense clearing and sanitizing standard – DoD 5220.22-M) when cleaning off hard drives.

Proper sanitizing usually involves a reformatting of the hard drive in a secure manner with an approved wipeout utility program. Degaussing software may need to be used to ensure total removal of files.

No hard drive will be reissued, sold or otherwise discarded until the drive has been sanitized.

- Media Re-Use. All e-PHI and other patient and business information shall be removed from any media devices before they are made available for reuse.
- Accountability. San Juan Island EMS tracks the movement of all computer hardware, workstations, and data storage devices. Movement both within the organization and outside the organization is tracked. A logbook is maintained to record the movement of all hardware and electronic media that is sanitized, reissued, or backed up and stored. The Information Security Officer oversees this accountability log.
- Data Backup and Storage. Each information system area will create an exact copy of all e-PHI when necessary immediately prior to any movement or disposal. This procedure is in addition to the standard routine backup protocol to ensure that all e-PHI is preserved before potential compromise.

XVIII. Electronic Information System Activity Review and Auditing

San Juan Island EMS is responsible for ensuring the privacy and security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

One aspect of our compliance program is to ensure that activity that takes place on our electronic information system can be “tracked” and documented so that quality assurance procedures will detect and address problems with the system. In other words, we need to be able to “look back” at our system and be able to identify the specific actions that have taken place such as timing and completion of back-up procedures, tracking server file access, and tracking power interruptions and other unusual events that could compromise our system and threaten the integrity of PHI and e-PHI.

Scope

This policy applies to all San Juan Island EMS staff members who are responsible for monitoring and maintaining our electronic information system or are responsible for its security. The policy also applies to staff members assisting with the audit and review process.

Procedure

1. The Information Security Officer will develop procedures to document use of PHI and e-PHI within the information system to track usage.
2. The Information Security Officer will review the records of information system activities, including a review of audit logs, security incident tracking reports, back-up records, etc.
3. Records of use will include, at a minimum:
 - a. The date of the use
 - b. A brief description of the PHI or e-PHI that was used
 - c. A brief statement as to what the PHI or e-PHI was used for and the disposition of that use
4. Uses need not be documented for purposes of an audit trail if the use is made entirely within the internal information system and the use did not involve any outside parties.
5. The manner in which the disclosures that are required to be logged under the Privacy Rule were made (PHI that is not related to treatment, payment or health care operations) shall be recorded and tracked.

Example: If the disclosure was made to a nursing facility by electronic mail, that fact should be documented as to when the transmission was made, the specific content of the transmission, who was responsible for requesting it, and who made the transmission.

XIX. Facility and Computer Access Point Controls

San Juan Island EMS is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Due to its critical importance to San Juan Island EMS, it is our obligation to control access to our physical locations, such as stations, buildings, garages and offices, as well as the rooms, vehicles, and secured areas where our electronic information system hardware, software, or other peripheral devices are stored or maintained. It is our policy to limit access to our electronic information system while at the same time, permit authorized access in the event of an emergency, or other events that require contingency plans to be placed in operation.

The contingency operations, facility security plan, and access and control and validation procedures are all part of facility and access point controls to preserve, protect, restore and limit or permit access to e-PHI. This policy describes our general approach to facility access under the Security Rule.

Scope

This policy applies to all San Juan Island EMS staff members who create, receive or use PHI and e-PHI, and any other confidential patient or business information. It is intended to cover all facilities that house our information system hardware, software and related devices and equipment.

Procedure

Contingency Operations

1. The Information Security Officer will work with managers of the electronic information system to determine contingency plans and procedures that should be implemented in the event of the need to restore lost data and to maintain uninterrupted access to e-PHI.
2. Working with management of the District, the Information Security Officer will develop a list of persons who have permission to access computer systems and secured areas in the event that restoration and preservation of data is necessary.
3. The Information Security Officer, as part of the contingency plan, will develop and maintain a list of persons authorized to have access to the facility when the contingency plan is in operation.
4. The Information Security Officer will work with management to develop a "call list" of persons who need immediate notification when the contingency plan is in operation.

5. The Information Security Officer will work with the communications center and other points of access to the facility to determine their role and procedures to follow in the event the contingency plan is in operation.

Facility Security

1. The Information Security Officer will work with management to determine who should have access to e-PHI and the electronic information system and determine the extent of that access.
2. Care will be taken to ensure that limitation of access does not hinder our ability to provide essential information needed for treatment and transport of patients, billing for our services, and health care operations.
3. An inventory of all software and hardware will be developed and maintained by the Privacy/Information Security Officer to include:
 - a. Assignment of identification numbers to hardware and other devices that are part of the electronic information system
 - b. A record book or file will be maintained to catalog all software and hardware, with their unique identification numbers. The inventory will be conducted on at least an annual basis.
 - c. Any discrepancies in the current inventory of software and hardware in comparison to the last inventory will be reported to management and will be investigated to ensure that there is a proper accounting of all SAN JUAN ISLAND EMS software and hardware.
 - d. A central storage area for all original/licensed copies of software, source codes, etc. shall be created that is secure and environmentally safe so that the software is protected from destruction or damage as best as possible.
4. All SAN JUAN ISLAND EMS staff members who are approved for access to e-PHI sources and the electronic information system shall be assigned unique passwords where appropriate to ensure secure access to the system.
5. The Information Security Officer will work with management to develop keypad access systems so that access codes may be changed when staff members leave the organization or the list of approved persons for access to the electronic information system has been changed.
6. There will be a list of all keys and passport devices issued to personal who have access to the electronic information system to ensure accountability.

The list will be developed and maintained by the Information Security Officer and updated as needed.

XX. Preserving Data and Electronically Stored Information: Creating Backups

Purpose

The purpose of this policy is to outline the procedures for preserving and protecting e-PHI and other important business information from tampering, theft, fire, flood, and other physical damage. A key to this process is the proper replication of exact copies of data in a secondary system so that if the primary system fails, the data will be completely preserved and accessible.

Scope

This policy applies to all electronically stored data and information created, received, used or stored by San Juan Island EMS. Creating backups will be the responsibility of the manager in charge of the particular computer equipment for his/her area of responsibility, in close coordination with the Privacy/Information Security Officer. This policy applies to all electronic equipment and storage devices that are owned or leased by San Juan Island EMS. The procedures apply to all staff members and vendors or contracted parties who are responsible for completing backups.

Procedure

Physical Access Controls

All backup systems will be located in a secure area, with limited access so that only those with responsibility for the backup system will have access to it. Servers, backup drives and other data and information saving hardware will be located in a locked room. The Privacy/Information Security Officer will maintain a current list of all individuals who are approved for access, and this list will be reviewed periodically.

Backup Schedule

Data and information stored on any computers or electronic devices will be backed up at the end of each work day whenever possible, but at a minimum, backups must be made at sufficient intervals to ensure that critical data (especially

PHI and e-PHI) can be restored and recovered immediately. A full system backup will be completed at least monthly.

All backup tapes, drives and other storage devices will be removed from the premises and stored at a secure off-site location on a weekly basis. This will ensure the preservation of all but the most recent data and information in the event of a catastrophic fire, flood, or other damage to the primary backup location.

There will be verification that the backup was successfully completed at the end of each backup process, to ensure that a complete replication of the data and information backed up has actually been created.

Backup Schedule Logs

The backup software will capture a list of all files and directories encountered and saved. Logs will be maintained and will contain information about successful backups, unsuccessful backups, backup media that was left in place accidentally and overwritten, when and where the media was sent off-site, the success or failure of restore tests and bad media encountered which may affect our ability to obtain files from a previous backup.

A primary and backup staff member will be assigned to rotate the media used for backups. This staff member will enter on the log at least the following information: 1) whether the backup was successful; 2) date and time the backup began and the date and time it was completed; 3) description of any problems encountered during the backup; 4) verification that a check was made to ensure that the backup was complete.

Marking and Storage of Backup Media

All backup disks, drives, tapes or other devices will be legibly and clearly marked with the fact that it is a backup, the date and time the backup was completed, and the initials or the staff member who completed the backup.

Backup devices and storage units will be stored in containers that help protect the backup from damage due to moisture or other environmental concerns.

Backup devices and storage units will be ultimately stored in a secure location and in cabinets or shelving that is conducive to its identification and protection within that location. Backup media will be stored in a manner that protects it from tampering, theft, fire, flood, and other physical damage.

Data Retention

Full system backups will be copied and/or archived at least weekly and will not be stored in the same geographic location as the source systems. Archived backups must be periodically tested to ensure that they are recoverable.

Off-Site Storage Procedures

All backups will be stored off site. San Juan Island EMS may contract with a reputable vendor to manage its backup process and media storage. The vendor must execute a Business Associate agreement with San Juan Island EMS to ensure that the vendor will, among other things, protect the integrity of the data stored and protect it from improper use or disclosure.

Security access controls implemented at the off-site backup and storage location must meet or exceed the security access controls of the source systems. In other words, information security at the backup storage location must equal or exceed the security where the primary computers and servers are located.

Documentation

The backup restore and recovery processes must be documented with the following critical information in accordance with the procedures established for maintaining paper (hard copy) backup logs. Backups must be performed in accordance with the documentation provided for the particular backup software or system.

Storage of Media Other Than Backups

Old hard drives or other media storage devices that have been removed from the information system will be handled as follows: 1) if the device is to retain data, it will be stored in a similar fashion as the backup devices; 2) if the device is to be taken out of service and no longer used to store data, it shall be "sanitized" and erased prior to disposal in accordance with industry standards.

Emergency Contact information

San Juan Island EMS will maintain a list of designated staff to be contacted in an emergency. A copy of this list will be kept in a secure location, such as the main computer facility and the off-site backup location. The list must be kept up to date and readily accessible in case of an emergency. The list will also include vendor contact and support information and contacts for the off-site media storage location.

XXI. Encryption and Decryption of e-PHI

Purpose

San Juan Island EMS is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Security involves protection of e-PHI, PHI and other important service information during its transmission and receipt via electronic means such as electronic mail and file, information, or software transfers. Encrypting and decrypting electronic information and files during their “transit” is a technical means of ensuring that if the information or files are intercepted or end up in the wrong hands, they cannot be deciphered or interpreted.

In effect, encryption turns the transmission into unique “gibberish” that transforms the electronic information or files into something that cannot be viewed in their original form unless it is decrypted at the receiving end. It is like attaching a unique “code” to that information so that it can only be accessed by those with the “de-coder.”

While we are not legally required to “encrypt” electronic information or files in most cases, we are obligated to ensure that e-PHI, PHI, and other important patient or service information does not fall into the wrong hands or is viewed or used by those who should not have access to it. Thus, it is the policy of San Juan Island EMS to use encryption or decryption techniques wherever possible.

Scope

This policy applies to all San Juan Island EMS staff members who are responsible for the manner in which e-PHI and other important District information is transmitted or received by the District.

Procedure

1. The Privacy/Information Security Officer will as part of a risk assessment identify all transmission and reception points for electronic information to determine:
 - a. Where the information is sent
 - b. The type of information that is sent

- c. The general content of the information to determine if it contains e-PHI or other important or confidential information
2. The Privacy/Information Security Officer in conjunction with management will then determine:
 - a. If the encryption and decryption of the information should be implemented based on the type of information, its destination (internal or external) and the risk of improper interception
 - b. If it is feasible to implement encryption and decryption of the information after a review of the costs of implementation
 - c. If implementation is not feasible, to document why it is not feasible
 - d. Establish other reasonable means to prevent the risk of improper access and use of e-PHI, PHI and other important confidential and District information if it should be intercepted by persons not authorized to receive it.
3. If encryption/decryption is implemented, a careful review of all available options will be completed by the Privacy/Information Security Officer, including a review of available technology, its features, and the ability to maintain and upgrade the software in the future.

XXII. Security Incident Management Policy

Purpose

Incidents that could compromise our electronic information system are serious as critical patient information may be damaged or lost. This policy establishes San Juan Island EMS's general policy on how to report a security incident and the steps that will be taken by the District to investigate and take action when a potential or actual security incident occurs.

Scope

This policy applies to all San Juan Island EMS staff members who utilize the electronic information system. It is everyone's obligation to know what to do when confronted with a security incident.

The "Computer Incident Reporting Form" (Form 32) should be used in conjunction with this policy.

Procedure

Security Incident Defined

A “Security Incident” is an attempted entry, unauthorized entry, or an information breach or attack on our electronic information system. It includes unauthorized probing and browsing of the files, a disruption of service from any cause, and incidents where electronic information has been altered or destroyed.

Security incidents may include such things as a virus or a worm, or unauthorized use of computer accounts and computer systems. It may also include complaints or reports of improper use of our information system.

Reporting a Security Incident

All staff members are responsible for immediately reporting a security incident or suspected security incident immediately.

When a suspected security incident occurs, a “Computer Security Incident Form” (Form 32) will be completed.

The Privacy/Information Security Officer will be responsible for initiating an immediate investigation to isolate the problem and take whatever action is necessary to protect the information system and e-PHI and other vital electronic information.

The Privacy/Information Security Officer will notify management immediately in the event the incident cannot be immediately corrected, or if any e-PHI or other vital information is altered or destroyed. Management will also be notified of any completed investigation and the outcome of the investigation. In the event of a suspected computer crime, or other unlawful activity via the use of the information system, local, state, or federal law enforcement may need to be notified. That determination will be made by management with recommendation from the Privacy/Information Security Officer.

Information Security Officer is responsible for coordinating communications with outside organizations and law enforcement.

Whenever a security incident, such as a virus, worm, hoax e-mail, discovery of hacking tools, altered data, or other event that could harm the information system is suspected or confirmed, remedial action will be taken, including action against any individual staff members when it has been confirmed that they caused or contributed to the incident.

Privacy/Information Security Officer Responsibility

The Privacy/Information Security Officer is responsible for the following:

- Initiating the appropriate incident management action, including restoration as defined in the Incident Management Procedures.
- Determining the physical and electronic evidence to be gathered as part of the incident investigation.
- Monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- Determining if a widespread communication is required, the content of the communication, and how best to distribute the communication.
- Communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- Initiating, completing, and documenting the incident investigation.

Enforcement

San Juan Island EMS's Privacy/Information Security Officer, office manager and supervisors are responsible for enforcing this policy. Staff members who violate this policy will be subject to disciplinary action, up to and including termination.

XXIII. Use of Computer and Information Systems Equipment

Purpose

San Juan Island EMS is committed to protecting our staff members, the patients we serve and the District 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 San Juan Island EMS. These rules are in place to protect the staff and patients of San Juan Island EMS. Inappropriate use exposes San Juan Island EMS 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 San Juan Island EMS 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 San Juan Island EMS.

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 San Juan Island EMS is at all times the property of San Juan Island EMS. Because of the need to protect the San Juan Island EMS computer network, the District cannot guarantee the confidentiality of information stored on any network device belonging to San Juan Island EMS, 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 District computer equipment. Please refer to the District's Policy on Preventing Sexual and Other Harassment for further information.
4. For security and network maintenance purposes, authorized individuals within San Juan Island EMS may monitor equipment, systems and network traffic at any time, to ensure compliance with all District 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, District 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 periodically in accordance with District policies.
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 San Juan Island EMS, shall regularly run approved virus-scanning software with a current virus database in accordance with District 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 San Juan Island EMS authorized to engage in any activity that is illegal under local, state, or federal law while utilizing San Juan Island EMS 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 service 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 San Juan Island EMS.
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 San Juan Island EMS 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 or PIN to others or allowing use of your account password by others. This includes family and other household members when work is being done at home.

6. Using a San Juan Island EMS computer device to actively engage in procuring or transmitting material that is in violation of the District'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, San Juan Island EMS staff members or patients to parties outside San Juan Island EMS.

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 San Juan Island EMS's networks of other Internet/Intranet/Extranet District providers on behalf of, or to advertise, any District hosted by San Juan Island EMS or connected via San Juan Island EMS'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 San Juan Island EMS. 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 District 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 District approval.
2. The District 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 District-owned remote devices for any purpose.
7. Remote device users will not install any software onto any PDA owned by San Juan Island EMS except as authorized by the District.
8. Users of District-owned remote devices will immediately report the loss of a remote device to a supervisor or 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.

XXIV. Use of Electronic Mail and Facsimile Transmissions

Purpose

San Juan Island EMS is responsible for ensuring the privacy and security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Electronic mail and facsimile transmissions are common methods for general communication and sending and receiving patient information. We need to ensure that e-mail and faxes are sent to the proper person and are received by the proper person.

In the event that e-mail and faxes are sent to or received by a person not designated to receive the information, it is important to provide notices and disclaimers on these transmissions to alert the receiving party that the transmission may be confidential and to give them steps they should take to alert us and to return the transmitted information.

Scope

This policy applies to all San Juan Island EMS staff members who use the electronic mail system or send documents by facsimile transmission.

Procedure

Electronic Mail

1. Electronic mail is intended to be used as a tool to facilitate communications and the exchange of information, including patient information that is needed to perform our Districts.
2. Occasional personal use is permissible so long as: (a) it does not consume more than a trivial amount of resources, (b) does not interfere with staff member productivity, (c) does not take priority over District business, d) and comports with our e-mail use and harassment policies.
3. In all cases, users of our electronic mail system have an obligation to use it appropriately, effectively, and efficiently.
4. Staff members must be aware that e-mail can be forwarded, intercepted, printed and stored by others. Therefore, users must utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.

5. E-mail accounts and passwords should not be shared or revealed to anyone else besides the authorized user(s).
6. All electronic mail transmissions that originate from San Juan Island EMS staff members must contain, at a minimum, a signature section that contains the following information:
 - a. The sender's full name
 - b. The name of the District
 - c. The telephone number of the District
 - d. An approved notice and disclaimer
7. Below the signature section, the following notice and disclaimer must appear on all transmissions from San Juan Island EMS staff members in at least 10 point font:

CONFIDENTIALITY NOTICE: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, and/or privileged information protected by law. If you are not the intended recipient, you may not use, copy, or distribute this e-mail message or its attachments. If you believe you have received this e-mail message in error, please contact the sender by reply e-mail and telephone immediately and destroy all copies of the original message.

Facsimile Transmissions

1. As with e-mail transmissions, the transmission of documents by facsimile machine requires similar protections and safeguards.
2. All facsimile transmissions must contain a cover sheet that includes at a minimum, the following information:
 - a. Name of the District
 - b. Name of the intended recipient
 - c. Name of the sender
 - d. Facsimile number of the recipient
 - e. Telephone number of the sender
 - f. Date of the transmission
 - g. The number of pages in the transmission
 - h. An approved notice and disclaimer
3. At the bottom of the facsimile cover sheet, the following notice and disclaimer must appear in at least 10 point font:

Confidentiality Notice: This facsimile transmission is confidential and is intended only for the review of the party to whom it is addressed. It may contain proprietary and/or privileged information protected by law. If you are not the intended recipient, you may not use, copy or distribute this facsimile message or its attachments. If you have received this transmission in error, please immediately telephone the sender above to arrange for its return.

Staff Member Personal Use of the Internet

Incidental personal use of Internet access is restricted to SAN JUAN ISLAND EMS staff members; it does not extend to family members or other acquaintances.

Incidental use must not result in direct costs to San Juan Island EMS.

Incidental use must not interfere with the normal performance of a staff member's primary duties.

No files or documents may be sent or received that may cause legal liability for, or embarrassment to San Juan Island EMS.

Storage of personal files and documents within San Juan Island EMS's information system should be nominal, and done only with prior approval.

All files and documents – including personal files and documents – stored on the electronic information system are owned by San Juan Island EMS and may be subject to review and monitoring, without your prior knowledge.

XXV. Staff Member Medical Records

Policy

To provide guidance to management and staff concerning the privacy and security of medical records which involve staff members of San Juan Island EMS.

Scope

This policy applies to all staff members to ensure the proper protection of that information so that no staff member inappropriately accesses another staff member's medical information, unless permitted by law or regulation. This policy applies equally to management and non-management staff members.

Procedure

San Juan Island EMS 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.

All staff member medical information will be kept in a locked office or a locked file cabinet. Any staff member medical information in electronic form will only be accessed by management personnel authorized and permitted under the law to access that information.

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 not 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 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, San Juan Island EMS 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 District's designated physician, and state agencies pursuant to state law.

With respect to staff members of San Juan Island EMS, 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 San Juan Island EMS provides ambulance service to an employee, the protections typically given to such information to our ambulance District patients applies to the employee. These protections are subject to HIPAA exceptions, such as in the situation in which the staff member used San Juan Island EMS District 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 San Juan Island EMS 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, San Juan Island EMS 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 San Juan Island EMS 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 San Juan Island EMS, please contact our Privacy Officer.