





Fire District 4 Policy & Procedure

Subject: HIPAA	Number: 114
	Effective: 09/14/2021
Fire Chief Approved: 	Supersedes: 114, 210, 211, 302, 303, 310
Commissioner Approval: 	Page 1 of 12
Legal Review By:	Date: 9/13/2021

1.0 **PURPOSE:**

- The District is responsible for patient information that we create, receive, share or use under the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HIPAA Omnibus Rule (2013).
- This policy outlines the roles and responsibilities of the Privacy Officer, Information Security Officer, Public Records Officer, Training Officer, Medical Services Officer, and Staff of Snohomish County Fire District 4 (SCFD4) with regards to the above regulations.
- The District, following the Privacy and Security Rule, will only disclose the minimum amount of patient information needed for disclosure. 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 treatment and transport of patients.
- Security of Public Health Information (PHI) and electronic PHI (e-PHI) is everyone's responsibility. This policy outlines the levels of access to PHI and e-PHI of various staff members of SCFD4 and provides policy and general procedures on access, disclosure, and use of PHI.

2.0 **PERSONNEL AFFECTED:**

This policy applies to all SCFD4 members who create, receive or use PHI and e-PHI and all other confidential patient or business information.

3.0 **PROCEDURE:**

3.1 **Privacy Officer Procedures**

Fire District 4 Policy & Procedure #412

- The Privacy Officer oversees all activities related to the development, implementation, and maintenance of SCFD4's policies and procedures covering patient health information privacy. This person serves as the compliance officer for all federal and state laws that apply to patient information privacy. The Privacy Officer and the Information Security Officer may be the same person.
- This position is responsible for 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.
- Responsibilities include, but are not limited to:
 - Working with the Training Division related to patient health information privacy and protected health information education for all members.
 - Assigning levels of access to PHI and minimum access requirements based on member's essential job responsibilities.
 - Acting as a contact person for dissemination of PHI to other health care providers.
 - Acting as HIPAA contact person for patient complaints and requests.
 - Ensuring fire department compliance with all applicable Privacy Rule requirements and working with legal counsel and other managers to ensure that SCFD4 maintains appropriate privacy and confidentiality notices, forms, and materials.
 - Overseeing all functions and staff related to HIPAA.
 - Convening, on at least an annual basis, a committee of managers and staff members to identify and review all existing policies and procedures for compliance with current laws and regulations regarding privacy.

3.2 Information Security Officer Procedures

- The Information Security Officer oversees all activities related to the development, implementation, and maintenance of SCFD4's policies and procedures covering electronic patient health information (e-PHI). This person serves as the vital compliance officer for all federal and state laws that apply to patient information

Fire District 4 Policy & Procedure #412

security, including the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Security Regulations under that law.

- This individual is responsible for 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. Their duties include but are not limited to the following:
 - Ensuring that the necessary and appropriate HIPAA related policies are updated and implemented to safeguard the security and integrity of all e-PHI used within SCFD 4 and provided to our business associates.
 - Ensuring the necessary infrastructure of personnel, procedures, and systems are in place to develop and implement the required HIPAA-related policies concerning the security of e-PHI.
 - Ensuring that the necessary infrastructure of personnel, procedures, and systems are in place to provide a mechanism for immediately reporting security incidents and HIPAA security violations.
 - Acting as a spokesperson and single point of contact for SCFD4 in all issues related to HIPAA security.
 - Periodically reviewing all security policies to ensure they maintain their viability and effectiveness.
 - Working with Training Division to ensure staff's educational programs are compliant with all e-PHI policies and procedures.
 - Cooperating with the state and federal government agencies charged with compliance reviews, audits, and investigations related to patient information security.
- SCFD4 retains strict requirements on the security, access, disclosure, and use of PHI and e-PHI. The use of PHI and e-PHI is based on the individual staff member's role in the organization. **Access to patient information is granted only to the extent needed to complete essential job responsibilities.**
- SCFD4's policy states that any activity taking place on our electronic information system must be "tracked" and documented so that quality assurance procedures will detect and address problems with the system.

Fire District 4 Policy & Procedure #412

- MDC/iPads or other electronic record mechanisms shall not be used or left in a place that the public can see the information (screen), unless the information is locked via the hardware or software security.
- Annual Security Assessment
 - The Information Security Officer will develop a process for completing an annual "walk through" of all areas where e-PHI is being used, stored, or transmitted.
 - The walkthrough will identify strengths and weaknesses in our current security compliance program and make recommended changes to update our process as needed.
 - The Information Security Officer will implement changes based on the results of this annual walkthrough and through information collected from other sources, such as staff members, other managers, business associates, and patients.
- Reporting a Security Incident
 - All members are responsible for immediately reporting a security incident or suspected security incident.
 - The 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 the Fire Chief immediately if the incident cannot be immediately corrected or if any e-PHI or other vital information is altered or destroyed. The Fire Chief 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 the Fire Chief with a recommendation from the Privacy/Information Security Officer.

3.3 Public Records Specialist Procedures

- The Public Records Specialist is responsible for maintaining Private Health Information (PHI) as required by Health Insurance Companies.

Fire District 4 Policy & Procedure #412

- This person will ensure that all HIPAA guidelines are used and followed during the patient's billing & auditing processes.
- The Records Specialist may access information only as part of duties to complete patient billing and follow up, and only while in the performance of one's assignment.
- There is no limit on a patient's access to their own PHI or e-PHI. Disclosures authorized by the patient are also exempt from the minimum requirements unless the District requests the authorization to disclose PHI or e-PHI.
- 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. If SCFD4 receives 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 necessary determination.
- Billing records, including but not limited to notes, waiver requests or other documents/records, should not be left out in the open. They should be stored in secure files and in an area with access limited to those who need access to the information to complete their job duties.
- It is the policy that only information contained in the Protected Health Information outlined in this policy is to be provided to patients who request access, amendment, and restriction on the use of their PHI under HIPPA.

Requests for Information:

- Upon presentation to the business office, the patient or appropriate representative will complete a Request for Public/Private Records form.
- The District must verify the patient's identity. If the requestor is not the patient, the requestor's name and reason for the request must be submitted in writing, along with an authorization request form signed by the patient. A copy of government-issued identification is acceptable for this purpose.
- The Records Specialist will act upon the request within fifteen days. Generally, the District must respond to requests for access to PHI within fifteen days of receipt of the access request. If the District is unable to respond to the request within this time frame, the requestor will receive a written notice explaining why the District could not respond within the time frame and provide a reasonable estimate of when the District will respond.

Fire District 4 Policy & Procedure #412

- The Designated Record Set should only include HIPAA covered PHI and should not include information used for the organization's operational purposes, such as quality assurance data, accident reports, and incident reports.
- The following reasons to deny access to PHI are not subject to review and are final, and cannot be appealed by the patient:
 - ❖ The information requested was compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding;
 - ❖ The information requested was obtained from someone other than a health care provider under a promise of confidentiality and the access asked would be reasonably likely to reveal the source of information.

Requests for an Amendment:

- The patient or appropriate requestor may only request an amendment to PHI contained in the Designated Record Set. Any request for amendment must accompany a "Request for Amendment of PHI" form.
- 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 period in which to comply by an additional 30 days.
- Once the Records Specialist grants the request for amendment, the requestor will receive a letter indicating that the appropriate amendment to the PHI or record has been made.
- The patient must provide written permission (authorization) so that the District may notify individuals with which the amendments need to be shared.
- The District will add the request for amendment, the denial or granting of the request, and any statement of disagreement by the patient, and any rebuttal statement by the District to the Designated Record Set.
- The District may deny a request to amend PHI for the following reasons:
 - ❖ The District did not create the PHI at issue;

Fire District 4 Policy & Procedure #412

- ❖ The information is not part of the designated record set;
- ❖ The data is accurate and complete.
- The District must provide a written denial, worded in plain language that includes:
 - ❖ The reason for the rejection;
 - ❖ The Individual's right to submit a statement disagreeing with the denial;
 - ❖ Directions on 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;
 - ❖ 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 the Secretary of Health and Human Services.

3.4 Training Officer Procedures

- Training Officers will ensure that all members understand the organization's concern for the respect of patient privacy and are compliantly trained in the District's policies and procedures regarding Protected Health Information (PHI) and the security of e-PHI.
- The Training 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.
- New staff members will receive training with updated privacy and security procedures, and HIPAA retraining upon employment and as otherwise necessary when updates to such procedures are made.
- Topics of the training will include a complete review of the District's privacy and security policies and procedures. They will consist of other information concerning the HIPAA Privacy and Security Rules, such as but not limited to, the following topic areas:

Fire District 4 Policy & Procedure #412

- 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).
- Description of protected health information (PHI) and electronically protected health information (e-PHI).
- Patient rights under the HIPAA Privacy Rule.
- Staff member responsibilities under the Privacy and Security Rules.
- The role of the Privacy/Information Officer and reporting employee and patient concerns regarding privacy issues.
- The Importance of and benefits of privacy compliance.
- The consequences of failure to follow established privacy and security policies.
- The use of the District's specific privacy and security forms.

3.5 Medical Services Officer Procedures

- The Medical Service Officer and the billing Coordinator are responsible for auditing the E.M.S. patient billing program in compliance with HIPAA.
- Access is granted only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel and the E.M.S. program.

3.6 Training Physician Procedures

- The Training Physician may access records only as a part of training and quality assurance activities. The Training Physician should redact all identifiable patient information before use in training and quality assurance activities.

3.7 Staff Procedures

- All staff members must adhere strictly to the password procedures established by the District.

Fire District 4 Policy & Procedure #412

- Staff are granted access only as part of completing a patient event and post-event activities, quality assurance checks, and staff's corrective counseling.
- 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.
- If the District needs to request PHI or e-PHI from another health care provider on a routine or recurring basis, the request must be limited to only the reasonably necessary information needed for the intended purposes of patient care and billing.
- Verbal and Physical Security
 - Common Areas: Staff members should only discuss patient care information with those who are involved in the care of the patient, regardless of their physical location. Staff should be sensitive to their level of voice and to the fact that others may be in the area. This approach is not meant to impede the ability to speak with other health care providers freely when engaged in the care of the patient. Staff should be free to discuss all aspects of the patient's medical condition, treatment provided, and any patient health information in their possession with others involved in the patient's care.
 - 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 viewing range of the monitor screen and take simple steps to shield viewing of the screen by unauthorized persons. All remote devices such as laptops and PDAs should remain in the physical possession of the individual to whom they are assigned at all times.

4.0 RESPONSIBILITY: SCFD 4 will appoint a Privacy Officer and Information Security Officer. It is their responsibility to be knowledgeable about Privacy and Security Rules.

5.0 DEFINITIONS:

5.1 PHI - Protected Health Information

5.2 e-PHI - Electronic Protected Health Information

5.3 HIPAA - Health Insurance Portability and Accountability Act of 1966

5.4 E.M.S. - Emergency Medical Service

Fire District 4 Policy & Procedure #412

5.5 Omnibus Rule (2013) - Implements many provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act

6.0 REFERENCE:

- 6.1** Federal HIPAA regulation 45 C.F.R. Sec.160, 162, and 164.
- 6.2** Breach Notification Rule of 2009
- 6.3** Final Omnibus Rule of 2013
- 6.4** Data Breach Policy 125

7.0 APPENDIX:

- 7.1** Request for Amendment for PHI Form
- 7.2** Request for Amendment of PHI Policy & Procedure Summary



Request for Amendment of PHI

Snohomish County Fire District 4

Patient Name: _____

Date of Birth: _____

Patient's Address: _____

Incident Date: _____

Incident #: _____

What is your reason for making this request?

Information to be corrected/amended:

Explain how the entry is incorrect /incomplete and what it should say to be more accurate/complete:

Do you know of anyone who may have received or relied on the information in question (doctor, pharmacist, health plan, health care provider, etc.) _____ YES _____ NO

If YES, please specify the name and address of the organization or individual:

Signature of patient

Date

FOR OFFICE USE ONLY

Date Received: _____

Amendment is:

Accepted

Denied

Signature of Public Records Specialist

If denied, check reason for denial:

- PHI not part of Designated Record Set
- SCFD4 did not create this record
- Record is accurate and complete
- Record unavailable under Federal Law

Fire District 4 Policy & Procedure #412



Request for Amendment of Public Health Information Policy & Procedure

Snohomish County Fire District 4

POLICY:

It is the policy of Snohomish County Fire District 4 (SCFD4) to permit an individual or their representative to request an amendment of their public health information (PHI) and for the request to be promptly viewed.

SCFD4 is required to act on the individual's request for an amendment no later than 60 days after receipt of the request. An extension of one 30-day period is allowed, provided that within the initial 60 - day period, the individual is notified in writing of the reason for the delay and the date by which action on the amendment will be completed.

SCFD4 is not required to agree to the amendment if the PHI or record that is the subject of the request:

- ◆ Was not created by SCFD4; ◆ Is not part of the designated record set; or ◆ Is accurate and complete.

PROCEDURE:

1. The Form **Request for Amendment of PHI** should be used for all requests for modification to an individual's public health information. This form is available on the District website, on the Records Request page.
2. The submit button at the bottom of the form will send it to the Records Request Officer, or it may be printed and mailed to RECORDS REQUEST OFFICER, 1525 Avenue D, Snohomish, WA 98290.
3. The Records Request Officer will review and log the request, and determine if it is to be accepted or denied.
4. If the amendment is approved (in whole or part) the following actions will be taken:
 - The Records Request Officer will send a signed copy of the request and notification of the amendment to all affected entities listed on the form. They will be notified of the amendment within 21 days of approval of the request.
 - The designated record set will include an appendage or link to the location of the amendment and its contents.
5. If the amendment is denied, in whole or in part, the individual has the right to send a written statement stating their disagreement with the denial and the basis for the disagreement. The statement should be sent to the Records Request Officer at the address listed in Procedure #2.
6. If the individual does not file a written statement disagreeing with the denial, they may instead send a written statement to the Records Request Officer for SCFD4 to provide the request for amendment and the denial with any future disclosures of their PHI.
7. The Records Request Officer will notify any individuals and/or organizations listed on the amendment, and all future disclosures will include this information.
8. SCFD4 may prepare a written rebuttal to the requestor's statement of disagreement and a copy of this rebuttal will be provided to the requestor.
9. The Requestor may file a complaint with Secretary of Health and Human Services: Umair A Shah, MD, 1700 E Cherry St Ste 200, Seattle, WA 98122.