

# Yamhill Fire Protection District

District Policies, Procedures, & SOG's

## MISSION

*Yamhill Fire Protection District is dedicated to  
serve and protect our community*

# District Procedure

## OPERATIONS

OPS-EMS – 508.1

## Patient Health Information Access, Security and Disclosure

Page 1 of 6

Issued: September 8, 2015

### ROLE BASED ACCESS

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

Job Title	Description of PHI to Be Accessed	Conditions of Access to PHI
EMT/ Firefighter	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
Fire Chief or his/her Designee		May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel

Access to PHI is limited to the above-identified persons only, and to the identified PHI only, based on the 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.

Access to a patient's entire file will not be allowed except when expressly permitted by District policy or approved by the Fire Chief or his/her designee.

# Yamhill Fire Protection District

District Policies, Procedures, & SOG's

## MISSION

*Yamhill Fire Protection District is dedicated to  
serve and protect our community*

# District Procedure

**OPERATIONS**

**OPS-EMS – 508.1**

**Patient Health Information Access, Security and  
Disclosure**

Page 2 of 6

**Issued: September 8, 2015**

## DISCLOSURES TO AND AUTHORIZATIONS FROM THE PATIENT

You are not required to limit your disclosure to the minimum amount of information necessary when disclosing PHI to other health care providers for treatment of the patient. This includes doctors, nurses, etc. at the receiving hospital, any mutual aid provider, your fellow crewmembers involved in the call, and any other person involved in the treatment of the patient who has a need to know that patient's PHI. In addition, disclosures authorized by the patient are exempt from minimum necessary requirements unless the authorization to disclose 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 to those entities, are not subject to the minimum necessary standards.

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

For all other uses and disclosures of PHI, the minimum necessary rule is likely to apply. A good example of when the minimum necessary rule applies is when the District conducts quality assurance activities. In most situations it is not necessary to disclose certain patient information such as the patient's name, address, social security number, all PHI of the treated patient, in order to conduct a call review. This sensitive information should be redacted or blacked out from the Patient Care Form being used as a Q/A example.

## DISTRICT REQUEST FOR PHI

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

# Yamhill Fire Protection District

District Policies, Procedures, & SOG's

**MISSION**

*Yamhill Fire Protection District is dedicated to  
serve and protect our community*

# District Procedure

**OPERATIONS**

**OPS-EMS – 508.1**

**Patient Health Information Access, Security and  
Disclosure**

Page 3 of 6

**Issued: September 8, 2015**

Holder of PHI	Purpose of Request	Information Reasonably Necessary to Accomplish Purpose
Skilled Nursing Facilities	To have adequate patient records to determine medical necessity for service and to properly bill for services provided	Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments
Hospitals	To have adequate patient records to determine medical necessity for service and to properly bill for services provided	Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments
Mutual Aid Ambulance or Paramedic Services	To have adequate patient records to conduct joint billing operations for patients mutually treated/transported by the 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 in the context of caring for a patient. The privacy laws were not intended to impede common health care practices that are essential in providing health care to the individual. Incidental disclosures are inevitable, but these will typically occur in radio or face-to-face conversation between health care providers, or when patient care information in written or computer form is left out in the open for others to access or see.

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

# Yamhill Fire Protection District

District Policies, Procedures, & SOG's

## MISSION

*Yamhill Fire Protection District is dedicated to  
serve and protect our community*

# District Procedure

**OPERATIONS**

OPS-EMS – 508.1

**Patient Health Information Access, Security and  
Disclosure**

Page 4 of 6

**Issued: September 8, 2015**

However, all personnel must be sensitive to avoiding incidental disclosures to other health care providers and others who do not have a need to know the information. Pay attention to who is within earshot when you make verbal statements about a patient's health information, and follow some of these common sense procedures for avoiding accidental or inadvertent disclosures:

## VERBAL SECURITY

### Waiting or Public Areas:

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

### Garage Areas:

Staff members should be sensitive to that 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.

# Yamhill Fire Protection District

District Policies, Procedures, & SOG's

## MISSION

*Yamhill Fire Protection District is dedicated to  
serve and protect our community*

# District Procedure

**OPERATIONS**

OPS-EMS – 508.1

**Patient Health Information Access, Security and  
Disclosure**

Page 5 of 6

**Issued: September 8, 2015**

## 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 a password only. Staff members should be sensitive to who may be in viewing range of the monitor screen and take simple steps to shield viewing of the screen by unauthorized persons. All remote devices such as laptops and PDAs should remain in the physical possession of the individual to whom it is assigned at all times. See the Yamhill Fire Protection District Policy on Use of Computer Equipment and Information Systems. See (PER 753.3A)

## PENALTIES FOR VIOLATION:

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

Staff members who do not follow our policies on patient privacy will be subject to disciplinary action, in accordance with Yamhill Fire Protection District Personnel Policy PER 749 or VOL 929.

# Yamhill Fire Protection District

District Policies, Procedures, & SOG's

## MISSION

*Yamhill Fire Protection District is dedicated to  
serve and protect our community*

# District Procedure

**OPERATIONS**

OPS-EMS – 508.1

**Patient Health Information Access, Security and  
Disclosure**

Page 6 of 6

**Issued: September 8, 2015**

## QUESTIONS ABOUT THIS POLICY OR ANY PRIVACY ISSUES:

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

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