| | | |
|---|---|---|
| | **UNIFIED FIRE AUTHORITY**<br>**ORGANIZATIONAL POLICY MANUAL** | |
| | Affiliation: Compliance and Records Division Policies | |
| | Title: **Security, Levels of Access**<br>Number: **200 – 100** | |
| | Approved: 6/13/2023 | By: Fire Chief Dominic Burchett |
| | Last Reviewed: 4/14/2025 | By: Shelli Fowlks Records Mgr. |

**DEFINITIONS:**
See UFA Policy and Procedure - General Compliance and Records Definitions

**LEADERS INTENT:**
The Health Insurance Portability and Accountability Act (HIPAA) requires a covered entity, such as UFA, to take reasonable steps to limit the use or disclosure of, and requests for, protected health information (PHI) to the minimum necessary to accomplish the intended purpose. This policy outlines UFA's commitment to adhere to HIPAA's minimum necessary standard. This policy outlines the appropriate levels of access to PHI that specific employees of UFA should have, identified as "Role Based Access." This policy does not in any way limit the amount of PHI that may be exchanged between UFA employees and other individuals involved in treating the patients.

**POLICY:**
UFA imposes strict requirements regarding the security, access, disclosure, and use of PHI. Access, disclosure and use of PHI is based on the role of the individual employee in the organization, and only to the extent that the person needs access to PHI to complete necessary job functions.

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

**PROCEDURE**

1.0 **ROLE BASED ACCESS**

1.1 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 identified persons need access, and any conditions, as appropriate, that would apply to such access.

See chart below:

| Job Classification | Description of PHI to Be Accessed | Conditions of Access to PHI |
|---|---|---|
| EMT/Paramedic | Dispatch information, EHR/PCR's, QA/QI reports | May access only as part of completion of a patient event and post-event activities and only while actually on duty |
| Records Manager/Compliance Officer | Dispatch information, EHR/PCR's, claim forms, and patient records from facilities | May access only as part of EHR/PCR review for billing, reconciliation, to fulfill legal requests, and only while actually on duty |
| Billing Clerk/Billing Company | EHR/PCR's, 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 |
| UFA Ambulance Committee Members | Billing records, hardship notices, and other patient records to determine eligibility for waiver | May access only as part of duties to determine hardship and only while on duty |
| Shift Captain, Shift Battalion Chief, Operations Chief, and EMS Division Chief | EHR/PCR's | 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 |
| EMS Division personnel responsible for QA/QI | Dispatch information, EHR/PCR's, QA/QI 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. This information may be accessed only while on duty |
| Command Staff | Dispatch information, EHR/PCR's, QA/QI reports, billing claim forms, and other patient information necessary for oversight | May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel and compliance with the law |
| Chief Legal Officer, Assistant Chief of Administration & Planning | EHR/PCR's, billing claim forms, remittance advice statements, all patient records | May access only to the extent necessary to monitor compliance and to accomplish appropriate management and compliance with the law |

## 2.0 DISCLOSURES TO AND AUTHORIZATIONS FROM THE PATIENT

2.1 UFA may disclose PHI to patients who are the subject of the information and to the extent authorized by the patient pursuant to policy. In addition, disclosures

authorized by the patient are exempt from the "minimum necessary standard" unless the authorization to disclose PHI is not in the best interest of the patient.

## 3.0 UFA REQUESTS FOR PHI FROM OTHER PARTIES

3.1 If UFA needs to request PHI from another health care provider on a routine or recurring basis, UFA must limit the requests to only the reasonably necessary information needed for the intended purpose, as described below. For requests not addressed in the table below, UFA will make this determination individually for each request, and in consultation with the Records Manager/Compliance Officer or Chief Legal Officer.

| **Holder of PHI** | **Purpose of Request** | **Information Reasonably Necessary to Accomplish Purpose** |
|---|---|---|
| Skilled Nursing Facilities | To have adequate patient records to treat the patient, 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 treat the patient, determine medical necessity for service and to properly bill for services provided | Patient information, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments |
| Mutual Aid Entities | To have adequate patient records to treat the patient, conduct joint billing operations for patients mutually treated/transports | EHR/PCR's |

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

## 4.0 INCIDENTAL DISCLOSURES

4.1 Incidental disclosures or unintended disclosures of protected health information (PHI) may occur during the course of permissible activities. HIPAA was not intended to impede common healthcare practices that are essential in providing health care to the individual. Incidental disclosures are inevitable, but these will typically occur in radio, face-to-face conversations between healthcare providers, or when PHI is viewed by others, despite reasonable efforts to protect PHI from view.

4.2 The Privacy Rule requires covered entities to minimize incidental disclosures of PHI by considering the circumstances and nature of the situation, along with the potential risks to PHI. Risks may be verbal, paper, or electronic. The

fundamental principle is that employees recognize the need to be sensitive to their surroundings while providing patient care to avoid accidental or inadvertent disclosures:

## 5.0 MEASURES TO PROTECT PHI

### 5.1 Verbal Security

5.1.1 Employees should only discuss PHI with those who are involved in the care of the patient, regardless of their physical location. When discussing PHI with patients, employees should take reasonable safeguard measures to ensure there are no other persons in the area that could overhear the discussion. Employees should be sensitive to the level of voice and to the fact that others may be in the area when they are speaking.

5.1.2 This approach is not meant to impede anyone's ability to speak with other healthcare providers freely when engaged in the care of the patient. When it comes to treatment of the patient, employees should be free to discuss all aspects of the patient's medical condition, treatment provided, and any health information they may possess with others involved in the care of the patient.

### 5.2 Physical Security

5.2.1 All paper patient records should be stored in safe and secure areas. No paper records concerning a patient should be left in open bins, open or unlocked vehicle cabs, 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 PHI paper records.

### 5.3 Electronic Protected Health Information

5.3.1 Computer access terminals and other remote entry devices such as tablets should be kept secure. Access to any computer device should be by password only. Employees 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 tablets should remain in the physical possession of the individual to whom it is assigned at all times.

Replaces policy dated: June 10, 2020