# Policies & Procedures

**Effective Date: 08/30/2012** **Article: 4.4**

**Revised Date:**

## PROTECTED HEALTH INFORMATION (HIPAA)

**PURPOSE:**

The following policy is a resource for the staff of Valencia County Emergency Services (VCES). These Guidelines are intended as a minimum set of expectations for confidentiality management.

VCES is dedicated to providing the best possible care to all patients. VCES will enforce policies that preserve the privacy and confidentiality of patient information to the full extent provided by the law, and that facilitate timely communication to continuing care physicians/facilities. Patient information will be stored and maintained in a safe and secure manner, and access to patient information will be limited to those specifically authorized. Access to patient information by those outside of the VCES is prohibited without the written authorization of the patient or unless otherwise permitted by law or regulation.

The VCES is required to fully document a patient's medical history, and other types of private information about patient's current condition, and all treatment rendered. This information is required to be maintained by the organization in a safe and secure way to protect privacy and confidentiality. The information must be available to those involved in the patient's care, but is restricted and is only accessed on a Need-to-Know basis. All other access is prohibited to the extent permitted by law without the patient's written authorization.

When access to patient information is permitted, such access may be made by viewing the original paper record, by obtaining a copy of the record, or by electronically receiving a transmission of the specified information on a Need-to-Know basis.

**Release of Medical Information**

The VCES will use a written authorization from the patient for the Release of Medical Information. The Release of Medical Information authorizes the VCES to release health information requested by third party liability entities related to the claims filed for specific dates of service. This statement also includes authorization for the release of medical information to other hospitals, physician(s), primary care physician(s), referring physician(s), or agencies in order to facilitate current care, to arrange ambulance transfers. All other access is prohibited without specific written authorization by the patient.

Certain medical data are needed in order to treat a patient and are not considered privileged data and do not require additional patient consent in order for the data to be transmitted to other caregivers who have a Need-to-Know. These data are:

- Patient's name
- Diagnosis
- Dates of Service
- Types of Service
- Medications
- Relevant behavioral material, e.g. elements of danger that other caregivers need-to-know.

**Principles for Medical Information Access/Release/Restriction**

- The right to access and to contribute to a patient's medical information is granted to staff if they are, have been, or will be involved in that patient's care. In this context, "staff" includes all ambulance personnel that participate actively in a patient's care
- Patients may have access to their records, within a reasonable period of time, as provided by state and federal law. Staff must insure that the patient has read and signed a Request for Release of Medical Records and has shown positive identification. If a guardian or power of attorney is requesting information they must provide their power of attorney papers and positive identification. The patient must be offered a copy of the signed Release. An incomplete request form is not valid.
- The patient has the right to revoke his request at any time. Staff must insure that the patient has read and signed a Revocation of Request for Release of Medical Records and has shown positive identification. If a guardian or power of attorney is revoking the request, they must provide their power of attorney papers and positive identification. The patient must be offered a copy of the signed Revocation.
- The patient has the right to request a restriction of uses and disclosures of their medical information. However, we are not required to agree to the request for restriction. If a patient wished to request a restriction of his medical record he must fill out a Request to Restrict Protected Health Information form. The form must then be given to the Fire Chief or designee who will make his decision and comment on the same form for chart documentation purposes.
- The patient has the right to revoke his request at any time. Staff must insure that the patient has read and signed a Revocation of Request to Restrict Protected Health Information and has shown positive identification. If a guardian or power of attorney is revoking the request, they must provide their power of attorney papers and positive identification. The patient must be offered a copy of the signed Revocation.
- A patient who disagrees with the accuracy of the information as presented in his/her medical record may make amendments to the medical record. Such amendments will be in the form of addenda to the record since changes and/or deletions in the original record are not allowed. The patient must sign a Request for Correction/Amendment to Health Information. The form must then be given to the EMS director who will make his decision and comment on the same form for chart documentation purposes.

Any access to patient's health information may be audited for appropriateness of access.

**Human Resource Management of Confidentiality**

The VCES has Human Resource policies that address confidentiality. These include, but are not limited to:

- A personnel policy that addresses confidentiality that includes a statement outlining corrective action that will be taken in the event of a breach of policy,
- A system for incorporating the VCES Confidentiality Policy into new employee orientation, e.g., discussion, distribution of policy,
- A signed statement by the employee stating they have read and understand the importance of confidentiality which will be placed in each employee's personnel file,
- A statement regarding confidentiality that is incorporated into job descriptions of those employees who routinely deal with confidential issues.

## PROFESSIONAL CONDUCT

Persons with access to information about a patient's medical history, and other types of private information about patient's current condition, and all treatment rendered, may only obtain information that is necessary to do one's job. ***Regardless of the format in which information is obtained,*** i.e., verbal, written, electronic or other technologic formats yet to be developed; it must be treated with the same level of confidentiality.

Viewing any information other than what is required to do one's job is a violation of the VCES Confidentiality standard, ***even if one keeps the information to oneself and does not disclose it to any other person and will lead to corrective action up to and including termination of employment and/or suspension and loss of privileges.***

***Persons who receive/view information about patients, employees, or business matters in order to do their jobs may not share the information with any others, unless the others need to know that information by virtue of their jobs.*** If a person needs to discuss confidential information with someone else as part of performing his/her job, he/she must be sure that the conversation is private and cannot be overheard. See Appendix C for the Employee Do's and Don'ts.

### Information Access

The VCES is required to fully document a patient's medical history, insurance coverage, and other types of private information about patient's current condition, and all treatment rendered. This information is required to be maintained by the organization in a safe and secure way to protect privacy and confidentiality. The information must be available to those involved in the patient's care, but is restricted and is only accessed on a Need-to-Know basis. All other access is prohibited to the extent permitted by law without the patient's written authorization.

***Need-to-Know*** is defined as that which is necessary for one to adequately perform one's specific job responsibilities. ***Access to a function on the computer does not imply that it is proper to search this information at will simply to satisfy curiosity.*** Hard copy records are accessed by request to the department responsible for safeguarding the document.

### Password Security Standards

Data available through this organization's information system are safeguarded by limiting access through personal passwords. **Access is determined by one's position, role, and/or responsibility. If a person's position, role and/or responsibility change, system access will be reevaluated as to its applicability**. If a password holder believes that someone else has access to their password, the password holder must take the proper steps to ensure that the password is changed. Further, the password holder should report the occurrence to the Security Administrator. Each Partners organization or practice should minimally have the following security standards in place:

- A designated written authorization process for granting of passwords and access. Such a process includes how the Password Administrator is identified. This Password Administrator is a specifically identified individual who grants others access to computer systems and functions within those systems.
- A system for annually (at a minimum) reviewing and amending those who have access to computer systems.
- A system that identifies the holder of the password through which each data inquiry, access and/or update is made, thus making it possible to determine information any given password holder has sought.
- A system to grant appropriate access to temporary personnel or outside staff, e.g., third party reviewers that allows for an automatic deactivation at specified time frames.

- A system to deactivate a user's password immediately upon termination or if a user's position, role and/or responsibility change.
- A system for instructing a new user:
  - Not to share his/her password or to inappropriately access information.
  - That each user is responsible for his/her password.
  - That each user is responsible for logging off the computer.

Additionally, the following safety precautions should be in place:

- Passwords are assigned with a minimum 5 or 6 alpha/numeric code.
- Passwords should not be re-used, even after their expiration.
- Passwords should be time-limited.
- Access should be granted, as appropriate, by varying levels of security.

**Electronic Communication:**

Staff must use electronic communication systems and devices including, but not limited to: electronic mail, fax machines, the internet, voice mail, cellular phones, in a way that protects the confidential information of others.

**Electronic Mail:**

Staff must use discretion in transmitting patient-identifying information by electronic mail. It is recognized that electronic mail is a vital form of communication and is used to facilitate the care process. ***When transmitting information via electronic mail or the Internet, the security of the transmission cannot necessarily be guaranteed.*** The patient's identity should be omitted in Internet communications. Staff should be aware that electronic mail communications are both hard to delete from the email system and may be subject to discovery in a lawsuit. The informality of electronic mail may lead staff to be more casual than they would otherwise be. However, electronic mail could be subpoenaed and introduced in a legal proceeding. Staff should take care in the tone and content of their communications on electronic mail

**Reproducing Patient Information (e.g. faxing, photocopying)...**

- Fax machines are the least controllable technology when one transmits patient information. It is critically important when faxing information that the sender has the correct fax number and that they know the receiving fax machine is in a secure location and/or that the intended receiver is available to immediately receive the fax.
- Fax cover sheets should contain the following wording:

"The documents accompanying this fax transmission contain confidential patient information belonging to the sender that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this patient information is prohibited from disclosing the information to any other party. If you have received this transmission in error, please notify the sender immediately and destroy the information that was faxed in error, and keep any information you may have viewed confidential."

- When receiving faxed patient information:
  - Immediately remove the fax transmission from the fax machine and deliver it to the recipient.
  - Manage patient information received via fax as confidential in accordance with policy.
- Destroy patient information faxed in error and immediately inform the sender by telephone or returned fax using the Fax Received in Error cover letter.

Questions about faxing patient information, or routine patient information requests should be sent the EMS Director.

**Requests from Outside Sources and/or Questionable Requests**

***All questions from the news media or other outside sources regarding patient information*** should be directed to the County Fire Chief's Office or the District Chief, unless the questions fall within the scope of one's own job description.

An employee who receives a request for information from a source he/she considers inappropriate should immediately report the request to his/her supervisor, who will take appropriate action.

**Manager Responsibility**

The County Fire Chief's Office and the District Chiefs ***should periodically review this policy with staff, monitor access to and distribution of information and act immediately on any suspected breach of confidentiality.***

## CONFIDENTIALITY: DOs and DON'Ts for EMPLOYEES

**Regarding Verbal Communication…**

- A patient's medical history, and other types of private information about a patient's current condition, and treatment should not be discussed where others can overhear the conversation, e.g. in hallways, in common rooms, at restaurants, at social events. It is not acceptable to discuss clinical information in public areas even if a patient's name is not used. This can raise doubts with the public about our respect for their privacy.

**Regarding Written Information…**

- Confidential papers, reports, and computer printouts should be kept in a secure place.
- Confidential papers should be picked up as soon as possible from copiers, mailboxes, conference room tables, and other publicly accessible locations.
- Confidential papers should be appropriately disposed of, e.g. torn or shredded, when they are no longer needed pursuant to the regulations set for the New Mexico Administrative Code.

**Regarding Employee Conduct…**

- Employees with access to information about a patient's medical history, and other types of private information about patient's current condition, and all treatment rendered to patients, may only obtain information that is necessary for job performance. **Regardless of the format in which information is obtained, i.e. verbal, written, electronic or other technologic formats yet to be developed; it must be treated with the same level of confidentiality**
- Accessing any information other than what is required to do your job is a violation of the VCES Confidentiality Policy, **even if you don't tell anyone else.**
- Accessing data must not occur simply to satisfy a curiosity. It is unacceptable to look up data, e.g. a friend's birthday, address or phone number. Information is only viewed when required for one's job.

**Regarding Computer Information…**

- Sharing a password instead of having your own password is prohibited.
- Passwords must not be written down where others can find and/or use them.
- Employees must not log on and let someone else use a computer under their password.
- Employees should protect their data and computer against unauthorized use by:
  - Using virus protection software.
  - Locking up backup diskettes or keeping them securely offsite.
  - Locking offices whenever possible
- Employees must log off the computer system when leaving a workstation.

**Remember…it is your responsibility to keep patient and hospital information - whether it is spoken, written, in a computer system, or just in your head - totally confidential.**

## Glossary of Terms

**Case Law:**
A body of law on a subject that derives from the resolution of court cases. Because it is the uncompiled outcomes of specific suits involving unique individuals and circumstances, case law is subject to varying interpretations and applications.

**Confidentiality:**
The right to rely on the trust or discretion of another; the right of an individual to control access to and disclosure of private information entrusted to another. Confidentiality arises in a relationship when an individual gives private information to another on the condition of or with the understanding that the other will not further disclose it, or will disclose it only to the extent that the individual directs.

**Consent:**
An individual's reasoned and voluntary agreement to something of a defined scope and purpose. Informed consent for medical treatment involves making an independent decision based on reasonable information of the risks and benefits of a particular procedure or treatment. Consent usually is express, either given in writing or by affirmative oral statement. It also may be implied by certain actions or inaction of the individual that lead others to a reasonable presumption about the individual's intent.

**Misidentified Information:**
Medical information which is anonymous, or from which identifying characteristics are completely removed. Misidentification requires the elimination not only of primary or obvious identifiers, such as the patient's name, address, date of birth, and treating physician, but also of secondary identifiers through which a user could deduce the patient's identity.

**Electronic Medical Records:**
A system of recording or retaining medical information in electronic form. As commonly understood, electronic medical records mean more than word-processed documents stored on an individual physician's computer, but rather an integrated and interactive system for storing records that can be accessed from remote locations.

**Information Privacy:**
The specific right of an individual to control the collection, use and disclosure of personal information.

**Least Necessary Privilege:**
Access to information and computer systems must be limited to those who legitimately need the data. To the greatest extent possible each individual's access to data should be limited to only what is necessary to accomplish the individual's work.

**Medical Information:**
Personal or private information that is reported at or derived from a clinician-patient encounter. In addition to medical history and treatment, medical information includes demographic, psychosocial, and behavioral information reported to or ascertained by a health care provider in the course of a patient visit.

**Privacy:**
The right to be left alone; the right of an individual to withhold himself and his property from public scrutiny. Privacy derives from the concepts of personal freedom and autonomy, and involves the ability of an individual to control the release or dissemination of information that relates to him/her.

**Regulations:**
Formal rules adopted by a government agency or department to implement uniform application of a statute. Although regulations are not themselves laws, they also are binding upon all persons to whom the statute applies.

**Security:**
Security encompasses all of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness and oversight of all of these areas. The purpose of security is to protect both the system and the information it contains from unauthorized access from without and from misuse from within. Through various security measures, a health information system can shield confidential information from unauthorized access, disclosure and misuse, thus protecting the privacy of the individuals who are the subjects of the stored data.

**Sensitive Information:**
Medical information for which the individual seeks heightened confidentiality protections. The determination of what is sensitive is unique to each individual, although certain categories of medical information are commonly recognized as potentially sensitive, such as mental health records, sexual history and orientation, sexually transmitted disease treatment, substance abuse treatment, etc. Information reported by an individual about family members or other persons should be considered sensitive for most purposes.

**Statute:**
A law that is the result of a formal action taken by a legislature. A statute governs all persons to whom it applies within the legislature's jurisdiction (i.e. federal or state). A statute may be a single act of the legislature or any number of related acts addressing one legal topic.

## PROTECTED HEALTH INFORMATION (HIPAA)

**EMS Field Provider's Guide to Request for Immediate Disclosure of Protective Health Information**

*Whenever possible, all requests for release of PHI should be routed through the Privacy Officer. When requests are made for immediate release of information, field providers may release information as outlined, only under the circumstances and to the individuals listed.*

| **IDENTIFYING INFORMATION** | | **DOCUMENTATION REMINDERS** |
|---|---|---|
| Name<br>Certificate/license #<br>Geographic identifiers (smaller than state)<br>Vehicle identifiers/Plate #<br>Device identifiers<br>Dates<br>Phone #<br>Fax# | E-mail address<br>Web sites (URLs)<br>IP address<br>Biometric identifiers (voice/finger prints)<br>Medical Record #<br>Health Plan #<br>Account #<br>Any other unique identifiers | 1. Document thoroughly any disclosures that are made.<br>2. If patient was given the opportunity to agree and /or object to disclosure, document this, using quotations whenever possible.<br>3. If patient was not given the opportunity to agree and/object to the disclosure, document the reason<br>4. Document the provider's considerations for deciding to make disclosure – why the provider feels the disclosure was appropriate. |
| **Disclosures to…** | **Reason (s)** | **Limitations** |
| Others involved in patient care, including BLS/ALS services, air ambulance services, receiving facilities, trauma centers, specialty treatment centers, etc. | Care/treatment of the patient. | None. "Minimum Necessary Rule" does not apply to treatment situation |
| Family members, friends and those involved in the care of the individual | 1. May disclose PHI to a family member, friend or other person identified by the individual relevant to that person's care or payment related to the care.<br>2. May disclose PHI to notify or assist in the identification or location of a family member | 1. May disclose location, general condition, death.<br>2. Must obtain patient's verbal agreement and/or give the patient the opportunity to object to disclosure. It's suggested to document that verbal agreement on the PCR.<br>3. If a patient is not present or can't agree or object, provider must determine based on professional judgment if disclosure is in the best interest of the patient and whether, based on the circumstances, the patient would likely agree to the disclosure if they could. |
| Coroner or funeral director | To identify a deceased person, determine cause of death or other duties as authorized by law. | May disclose PHI to coroner, medical examiner or funeral directors for the reasons listed. |
| Government authority, Social Security agency or other agency authorized by law | If you believe a patient is the victim of abuse, neglect or domestic violence (except children-refer to "pursuant to process and as otherwise required by law" under "Disclosure to Law Enforcement") | May disclose PHI if the victim agrees to the disclosure, OR disclosure is expressly authorized by law, AND the provider believes disclosure is necessary to prevent serious harm to the individual or other potential victims.<br>If the patient can't agree due to incapacity, may disclose if the information is not intended to be used against the victim.<br>If the disclosure is made, must promptly inform the patient that disclosure has been or will be made, UNLESS informing the individual would place the patient at risk of serious harm, OR you would be informing a personal representative may be responsible for the abuse, neglect or other injury and informing such person would not be in the best interest of the patient. |
| Avert a serious threat to health or safety. | 1. Disclosure is necessary to prevent or lessen a serious and imminent threat to health or safety of a person or the public.<br>2. An individual admits participation in a violent crime.<br>3. It appears that the individual has escaped from a correctional institution or lawful custody.<br>4. Disclosure is necessary for law enforcement to identify or apprehend a suspect. | May disclose necessary information to person or persons reasonably able to prevent or lessen the threat (including the target of the threat) |

| Disclosures to: | Reason (s) | Limitations |
|---|---|---|
| Employers | The provider provides health care to the individual at the request of the employer PHI consists of findings concerning a work-related illness or injury.<br>The employer needs the PHI to comply with its obligations regarding workplace medical surveillance (e.g., OSHA) | The provider must provide written notice to the individual that PHI was released to the employer. |
| Law Enforcement | Pursuant to process and as otherwise required by law.<br>Court orders, warrants, subpoenas, summons, Grand Jury subpoena.<br>Reportable injuries required by law (e.g., gunshot, stabbing, child/elder abuse, animal bite, etc, specific to state law_ | According to state law. |
| | Identification or location of a suspect fugitive, missing person or material witness. | May release only name, address, date and place of birth, SS#, blood type, type of injury, date and time of treatment, date and time of death (if applicable), distinguishing physical characteristics (height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, tattoos). |
| | Victim of a crime | Patient must agree to disclosure<br>If patient can't agree due to incapacity or emergency circumstances, provider must ensure that:<br>**a) *Information*** is needed to determine whether a violation of law by a person other than the victim has occurred and that the information is not intended to be used against the patient.<br>**b) *Immediate*** law enforcement activity depending upon disclosure would be adversely affected by waiting until the individual is able to agree to disclosure.<br>**c) *Disclosure*** is in the best interest of the individual based on the best professional judgment of the provider. |
| | Decedents | May disclose information to law enforcement about an individual who has died if you suspect that the death may have resulted from criminal conduct. If the death is not suspected to be crime-related, may not report to law enforcement unless required by law. May report to coroner or funeral director (see "Disclosures to Coroner or funeral Director") |
| | Crime on premises | May disclose PHI that you believe in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity. |
| | Reporting crimes in emergencies. | In an emergency situation, may disclose PHI to a law enforcement official if disclosure appears necessary to alert law enforcement to the commission & nature of a crime, the location of such crime or victim of such crime, the identity, description and location of the perpetrator of such crime. |
| | Inmate of a correctional facility or patient in police custody (e.g., patient under arrest). | May disclose PHI to institution or official if PHI is necessary for :<br>Provision of health care to the patient.<br>The health & safety of the patient or other inmates<br>The health & safety of the officers, employees or others at the correctional institution.<br>Law enforcement on the premises of the correctional institution.<br>The administration and maintenance of the safety, security, and good order of the correctional institute. |

Company name: _____

Privacy officer: _____

Contact number: _____

## Employee Confidentiality Agreement

The VCES has a legal obligation to safeguard the privacy of all patients and to protect the confidentiality of their health information. Additionally, the Valencia County Emergency Services (VCES) must assure the confidentiality of its computer systems, and management information. In the course of my employment/assignment I may come into the possession of confidential information*. In addition, my personal access code ["USER ID(s)" and PASSWORD(s)] used to access computer systems is also an integral aspect of this confidential information.*

By signing this document I understand the following:

1. I agree not to disclose or discuss any patient's medical history, insurance coverage, and other types of private information about patient's current condition, and treatment rendered with others, including friends or family, who do not have a need-to-know.
2. I agree not to access any information, or utilize equipment, other than what is required to do my job, even if I don't tell anyone else.
3. I agree not to discuss a patient's medical history, insurance coverage, and other types of private information about patient's current condition, and treatment rendered where others can overhear the conversation, e.g. in hallways, in common rooms, at restaurants, at social events. It is not acceptable to discuss clinical information in public areas even if a patient's name is not used. This can raise doubts with the public about our respect for their privacy.
4. I agree not to make inquiries for other personnel who do not have proper authority.
5. I agree not to willingly inform another person of my computer password or knowingly use another person's computer password instead of my own for any reason.
6. I agree not to make any unauthorized transmissions, inquiries, modifications, or purging of data in the system. Such unauthorized transmissions include, but are not limited to, removing and/or transferring data from the VCES computer systems to unauthorized locations, e.g. home.
7. I agree to log off prior to leaving any computer or terminal unattended.

I have read the above special agreement and agree to make only authorized entries for inquiry and changes into the system and to keep all information described above confidential. I understand that violation of this agreement may result in corrective action, up to and including termination of employment and/or suspension and loss of privileges. I understand that in order for any "USER ID" and/or PASSWORD to be issued to me, this form must be completed. I further understand that computer access activity is subject to audit.

_____ _____
Signature of Employee Date

_____ _____
Signature of Witness Date

To Be Filed in Employee's Personnel Record