ELECTRONICALLY TRANSMITTED INFORMATION

It is the policy of CITY OF CALEXICO to utilize electronic security mechanisms to ensure the validity of the information being electronically transmitted or stored.

PROCEDURE:

- The computer system has an integrated automatic encryption program installed.
- This program automatically activates when specifically identified information is accessed for electronic transmission.
- The encryption program prevents the interception of confidential patient healthcare information by unauthorized parties or computer systems.
- Information that is being electronically transmitted:
    - Select the information to be transmitted.
    - Select the appropriate “send” mechanism to transmit the information.
    - Await confirmation if the information sent was “completed” or “incomplete”.

DELIVERY, REMOVAL AND TRANSMISSION OF INFORMATION

It is the policy of CITY OF CALEXICO to secure and maintain the confidentiality of all patient healthcare information during the delivery, removal and transmission of the information.

PROCEDURE:

- Employees of Information Services are responsible for:
    - Logging when confidential information was accessed and for what purpose. Purposes include: data backup procedures, data storage, disposal.
    - Performing the intended purpose for accessing the information.
        - Data Backup: Create electronic tape backups of the computer systems.
        - Data Storage: Labeling the data backup tapes; ensuring safe delivery of the tapes to the off site storage facility.
        - Data Disposal: Ensuring all confidential healthcare information is removed or otherwise secured; contacting appropriate business to request the removal of used/damaged/replaced computer hardware.
    - Documenting the accessing of the information, the purpose for accessing the information and the final disposition of the information.
    - Reporting to the Director of Information Services any deviations from this plan.

PHYSICAL SAFETY

It is the policy of CITY OF CALEXICO to ensure the physical safety of all confidential patient healthcare information. In doing so, CITY OF CALEXICO has assigned responsibilities to manage the security of this information.

PROCEDURE:

- The Director of Information Services is responsible for the management and supervision of all personnel within the Information Services Department.

- The personnel within the Information Services Department are responsible for:

    - Maintaining the security and confidentiality of all computer systems.

    - Refusing access to individuals requesting access to confidential patient healthcare information without the appropriate authorization.

    - Reporting attempts made to access confidential healthcare information without the appropriate authorization.

SECURITY TRAINING

It is the policy of CITY OF CALEXICO to train all employees on the measures taken to ensure the security of confidential patient healthcare information.

PROCEDURE:

- Upon hire, every CITY OF CALEXICO employee receives information security awareness training in orientation to include:
    - How to use specific computer applications needed to perform the work for the position in which they are employed.
    - Access code confidentiality and password maintenance.
    - Monitoring of ability to log-in and reporting of failure to log-in events.
    - Efforts to maintain the sterility of the computer environment to include firewalls to trap viruses and unauthorized transmittal of confidential healthcare information between and among other unauthorized computer systems.
        - In the event of a virus, the employee is to contact the Department of Information Services and report the virus.
        - The Department of Information Services will communicate the status of the virus and notify all departments when the virus is removed.
    - Limits of CITY OF CALEXICO e-mail to be within and among identified departments.
    - Sanctions against the loading and use of unauthorized personal software programs to include screen savers, games, Internet access and any other such programs that would hinder the productivity of patient care.
    - Documentation of Security Management Training is kept in the Information Services Department and copied to the employee's personnel file.
- Information security management updates are to be provided as part of the CITY OF CALEXICO's yearly employee information review and as needed. Elements of the initial orientation training are reviewed. Documentation of attendance at an update session is kept in the Information Services Department and copied to the employee's personnel file.

TERMINATION

It is the policy of CITY OF CALEXICO to uphold the security of all confidential patient healthcare information when an employee is terminated from the CITY OF CALEXICO or at the ending of a business association.

PROCEDURE:

- Upon notification of an employee's termination from employment at CITY OF CALEXICO, the following is done:
    - Department manager will notify the Director of Information Services of the employee's termination date.
    - Employee's department manager will provide the location of any locking mechanisms in which the employee had access.
    - The Director of Information Services will notify the manufacturer of the locking mechanisms of the need to change the access combination or lock.
    - The Director of Information Services will locate the departing employee's name on the Access Code List and will delete the employee from the active list roster.
    - The Director of Information Services will electronically deactivate the employee's access code on the last day of employment.
    - The Director of Information Services will notify those departments in which the employee had access through keys, tokens or access cards so that all access privileges can be deactivated.
    - Employees refusing to relinquish items used to secure confidential patient healthcare information will be reported to law enforcement officials.
    - Documentation of items received from the employee will be placed in the Information Services Department and in the employee's permanent record of employment with CITY OF CALEXICO.

- The security management process is evaluated and reviewed annually by the appropriate committees.

- Documented changes to the security management process will be communicated to all employees on a routine basis.

- The Information Services Department is responsible for ensuring all employees have been notified of any changes to the Security Management Process to include the name of employee and date of training.

PROCEDURE:

- The Director of Information Services is responsible for overseeing the integrity of the security management process.

- The Security Management Process includes:

  - Roles and responsibilities of the Director of Information Services to include overseeing the implementation of security policies, employee education regarding security measures, integrity of electronic communication, the physical security of the information and decisions regarding the abuse or misuse of the information.

  - CITY OF CALEXICO employees are trained on the security measures regarding confidential patient healthcare information. This information is provided upon initial orientation to CITY OF CALEXICO as a new employee and reviewed annually by the Trainer and the Information Services Department. Documentation of the original information and the annual review is kept in the Information Services Department.

  - CITY OF CALEXICO employees found breaching the confidentiality of patient healthcare information will be placed in the disciplinary process to include:

    - First Offense - Verbal Warning; documentation of such will be placed in the employee's permanent record.

    - Second Offense - Written Warning; documentation of such will be placed in the employee's permanent record.

    - Third Offense - Limited use of access code only upon supervision from the department manager; placed on probation for three (3) months; documentation of such will be placed in the employee's permanent record.

    - Fourth/Final Offense - Termination of employment; documentation of such will be placed in the employee's permanent record; notification to appropriate licensure boards of violation of confidential patient healthcare information.

  - Business associates/subcontractors of CITY OF CALEXICO are expected to maintain the confidentiality of patient healthcare information. If found in violation of this confidentiality, the following will occur:

    - Provide notice of civil or criminal penalties for misuse or misappropriation of healthcare information.

    - Violations may result in notification to law enforcement officials, regulatory agencies or accreditation agencies.

    - Limit use of system privileges or cease all use of system privileges.

    - Enforce violation of contract penalties.

BREACHES OF SECURITY

It is the policy of CITY OF CALEXICO to monitor and report any breaches of security to confidential patient healthcare information.

PROCEDURE:

- The Director of Information Services receives notification of a breach of security to confidential patient healthcare information. This breach is reported via the Employee Login Access Report or through direct observation.

- The Director of Information shall report the breach of security to the Privacy Officer to keep a log of the breaches and discipline.

- The Director of Information Services or designee contacts the department manager of the employee responsible for the security breach.

- The Director of Information Services or designee and the department manager meet with the employee to review the information regarding the breach.

- The employee is given an opportunity to discuss the breach with the Director of Information Services or designee and the department manager.

- Upon completion of this discussion, the Director of Information Services or designee and the department manager determine the degree of employee sanctions needed.

- The Director of Information Services or designee and the department manager will review the amount, quality and volume of information breached.

- The Director of Information Services or designee and the department manager documents the investigation of the breach, employee sanctions and results of the breach. This information is housed in the Information Services Department.

- It is the policy of CITY OF CALEXICO to manage the security of all confidential patient healthcare information.

- CITY OF CALEXICO believes that all patient healthcare information is confidential and must be kept in a secure manner. CITY OF CALEXICO upholds the highest level of security of all confidential patient healthcare information. In the event of any breaches of this security, CITY OF CALEXICO will strive to recover the information released in the breach, identify the employee(s) responsible for the breach and discipline those responsible for the breach.

- Scanning the computer system for presence/absence of viruses.
- Scanning the computer system for virus code fragments.
- Scanning the computer system for other “like” virus fragments to include worms and Trojan horses.
- Documenting the outcome of the scan for viruses, worms and Trojan horses.
- Maintaining the documentation from the virus scans in the Information Services Department.

COMPUTER SOFTWARE

It is the policy of CITY OF CALEXICO to utilize measures to ensure the security of confidential patient healthcare information located within the computer software programs of the organization.

PROCEDURE:

- The Director of Information Services or designee is responsible for the ongoing maintenance of the computer software programs.
- A complete list of computer software programs is kept in the Information Services Department.
- Written instructions/directions for each computer software program are kept in the Information Services Department.
- Each program is reviewed monthly for:
    - Installation procedures
    - Connection procedures
    - Updating with software releases procedures
    - Loading new software procedures
    - Efficacy of security procedures
    - Virus checking
- Each software program is tested monthly for adequacy of security measures. This monthly testing includes:
    - Validation of its use in the intended environment.
    - Documentation of attempts to violate the security of the software.
    - Documentation of the results of the attempts to violate the software's security.
    - Documentation of the remediation if the software's security was violated.
    - Documentation of any customer service support help enlisted in response to violations made to the software's security.
- Each software program is tested monthly for adequacy of virus scanning. This monthly testing includes:

- Computer access codes are to be utilized by the employee assigned to the code. Sharing of computer access codes is grounds for disciplinary action. Sharing of access codes may result in the loss of access to the computerized system.

SECURITY

It is the policy of CITY OF CALEXICO to secure all confidential data and information throughout the organization. All individuals expected to utilize computer systems will be assigned an access code.

PROCEDURE:

- All individuals expected to utilize the CITY OF CALEXICO computer system are assigned an access code known only to the members of the Information Services Department and the employee.

- Employees of the Information Services Department are prohibited from displaying, accessing or reviewing the employee listing of access codes without authorization or supervision from the Director of Information Services. Employees of the Information Services Department are trained in the need to maintain the confidentiality of the access codes information. Any Information Services Department employee found in violation of this security measure will be placed in CITY OF CALEXICO's disciplinary process.

- A master listing of employee access codes is kept in an electronic file in the Information Services Department. This file is password protected. A backup file is available in the off-site storage facility. The Director of Information Services or designee is responsible for updating the employee access codes file on a monthly basis, creating the back up file and storing in the off-site storage facility.

- Prior to assigning employee access codes, each employee attends computer training.

- Upon completion of this training, the Trainer, Information Services Department completes the security access code form and submits it to the Information Services Department to assign the employee a permanent computer access code. The form is completed in its entirety by the Trainer prior to assigning an access code and includes the following information:

    - Name of employee requesting an access code and initials

    - Employee identification number

    - Employee signature confirming acceptance of "Confidentiality of Information" statement

    - Employee signature confirming acceptance of confidentiality of access code

- The employee is assigned a code which is effective immediately upon receipt of the confirmations of confidentiality of access code signature.

LEVELS OF ACCESS OF CONFIDENTIAL INFORMATION

- It is the policy of CITY OF CALEXICO to determine the need for access to and appropriate levels of security and confidentiality of healthcare information. Individuals/departments are identified with specific policies/procedures defining the degree of access and need for healthcare information.

    - Information Services Department personnel will have access to all documentation present in the medical record.

    - Nursing personnel will have access to all pertinent patient information to allow for optimum assessment, treatment and care of the patient in accordance with general nursing policies and procedures.

    - Claims staff will have access to all pertinent patient information that will allow them to provide claim processing.

    - Clerical personnel categorized as business office will have access to all necessary patient information that allows for appropriate insurance procedures.

    - Performance Improvement, Utilization Review, Case Management and Risk Management Department personnel will have access to all pertinent patient information, both clinical and financial, to allow for optimum assessment to perform the expected function within the department.

    - All other ancillary and administrative personnel will have access to patient information on an as needed bases, restricted to level of authority, according to policies and procedures which govern the security and confidentiality of patient information.

    - Once degree of access has been established, the employee is issued a log-in and passcode to use when accessing the medical record by the Information Services Department. The Information Services Department controls the degree of access of computerized medical records by electronically granting privileges to portions of the record and subsequent database.

    - In the event any employee's status changes or upon voluntary or involuntary termination, the Information Services Department will reset the electronic authorization privileges or electronically restrict access. Employees who attempt to access any portion of the medical record outside of the identified privilege area will be notified of a "restricted access" message. An electronic log entry will be created in the Information Services Department for review by the Director. This report will be submitted to the Privacy Officer for review and action as appropriate.

INTEGRITY OF CONFIDENTIAL INFORMATION

It is the policy of CITY OF CALEXICO to maintain the integrity of confidential healthcare information.

PROCEDURE:

- Confidential patient healthcare information is inputted directly into the computer system. In the event of a hard copy of the medical record, the records shall be maintained in a secure environment and not left unattended in areas accessible by nonauthorized individuals.

- The Information Services Department's main door shall be locked at all times. Access to the department will occur by those personnel with access to the security code on the door lock (or other electronic mechanism such as a code key or physically by a receptionist in the event the area does not have an electric security lock).

- The medical records stored in the CITY OF CALEXICO will be secured so that damage from fire or water will be minimized. Records may be housed in mobile fire-resistant cabinets or other protective devices.

    - Disposal of damaged paper medical records will be by incineration or shredding. Residue from shredding will be removed by a reputable waste removal company for incineration off-site.

- Electronic records will be maintained according to the electronic records back-up and storage policy.

- The Information Services Department is responsible for safeguarding the electronic record and its contents again loss, defacement and tampering. This department is also responsible to safeguard the medical records against use by unauthorized individuals or personnel.

    - Disposal of damaged electronic information will be conducted so that the information is completely incinerated.

- The medical record is the property of the hospital and is maintained for the benefit of the patient, the medical staff and the hospital. Authorization to access the medical record for anything other than patient care must obtain authorization from the Director of Information Services or designee.

- The outcome of each test is documented and matched with the established plan and procedure.
- Changes are made to the plans or procedures as identified from the testing.
- Documentation of the testing is maintained by the Privacy Officer.

- ◊ The Director of Information Services or designee will contact Customer Support Department and report the situation.
- ◊ Direction will be taken by the Customer Support Department.
- ◊ Obtain back-up tapes from off-site storage facility to install in preparation to maintain operations.
- ◊ Employees are to revert to the use of manual patient information collection and documentation until a contingency computer system has been installed.
- ◊ Manually collected patient information and documentation will be inputted into the contingency system immediately upon resolution.

- Emergency Mode Operations:
  - Policy:
    - The emergency mode operations plan is implemented in the event of a fire, vandalism, natural disaster or system failure.
      - ♦ Notify the Director of Information Services of an emergency.
      - ♦ If possible, ensure the security of the electronic information by closing doors and restricting access except to personnel authorized by the Director of Information Services and the Privacy.
      - ♦ Determine the effects of the emergency and implement the appropriate plan: fire, vandalism, natural disaster, system failure.
      - ♦ Maintain the selected emergency plan until the emergency is resolved or a contingency plan is implemented to maximize operations.

- Testing and Revision Procedures:
  - Policy:
    - System emergency plans and procedures are tested every two (2) months.
      - ♦ The Director of Information Services creates a schedule to test each emergency plan and procedure.
      - ♦ Each plan is test in a controlled environment.

- If necessary, obtain back-up tapes from off-site storage facility and input them into the system.

- Utilize all available resources to resume and maintain operations.

♦ System Failure: In the event of a system failure, the following is to be done:

- Establish the integrity of the Information Services Department.

- Determine the degree of information in the computer system at the time of the system failure.

- The Director of Information Services will determine the amount of information loss, if any, from the failure.

- The Director of Information Services or designee will notify all effected departments of any information lost to allow for appropriate retrieval of information.

- If the Information Services Department is intact:

  ◊ Notify the Director of Information Services or designee if the failure occurs during off hours. This individual will in turn notify all other employees of effected departments of the system failure.

  ◊ Employees are to revert to the use of manual patient information collection and documentation until the computer system failure has been resolved.

  ◊ Manually collected patient information and documentation will be inputted into the electronic system immediately upon resolution of the system failure.

- If the Information Services Department is not intact:

  ◊ Notify the Director of Information Services immediately.

  ◊ The Director of Information Services will assess the situation immediately of the degree of damage.

  ◊ The Director of Information Services or designee will notify all other personnel of affected departments as soon as possible.

- Ensure that no employee is in immediate danger.
- Close the doors around the fire area.
- Sound the alarm by pulling the fire alarm and notifying the operator and giving the physical location of the fire.
- Unplug all electrical equipment.
- Secure all confidential records inside a fire-resistant storage cabinet.
- Remove as much portable equipment as possible.
- Maintain personal safety.
- Await confirmation from Fire Department personnel before returning to the fire location and resuming operations.

♦ Vandalism: In the event of vandalism, the following is to be done:

- Request that nothing be touched in the area affected by vandalism.
- Notify Security immediately.
- Secure the site of the vandalism.
- Provide inventory of information, data and equipment that was vandalized.
- Await confirmation from Security personnel before resuming operations.

♦ Natural Disaster: In the event of a natural disaster, the following is to be done:

- Ensure safety of all personnel.
- Secure the region by closing all available doors or erecting barriers around the area.
- Conduct an inventory of information, data and equipment that was damaged.
- Identify needs for replacement of information, data and equipment.

SECURITY

It is the policy of CITY OF CALEXICO to secure electronic data from damage or loss.

PLANS TO RESPOND TO A SYSTEM EMERGENCY:

- Applications Criticality Analysis:
  - Policy:
    - All computer software applications are analyzed to ensure the integrity of the stored information.
      - Every computer software application is assessed monthly for the integrity of firewalls, pass codes, passwords, storage capacity and transmission capabilities.
      - Documentation of the monthly assessments are maintained by the Privacy Officer.
- Data Backup Plan:
  - Policy:
    - Protection of computer data is performed through a back-up for stored information.
      - Entire system is copied onto magnetic tapes each evening as part of the nightly system shutdown procedure. There are no exceptions to this process.
      - Nightly back-up tapes are rotated on a daily basis, 7 days per week, 365 days per year.
      - All back-up tapes are stored off-site in a fire resistant enclosed container.
- Disaster Recovery Plan:
  - Policy:
    - There is a plan to maximize the confidentiality of information and to maintain operations in the event of a disaster to include fire, vandalism, natural or system failure.
      - Fire: In the event of a fire, the following is to be done:

CERTIFICATION PLAN

- The Director of Information Services is to provide a list of all computer systems within CITY OF CALEXICO.
- List the elements to be evaluated for maximum security.
- Review the criteria to evaluate the security of the computer systems.
- Conduct a practice certification to evaluate the current status of the computer systems.
- Analyze the results of the practice certification to determine areas of deficiency.
- Correct any deficiencies.
- Conduct a follow-up practice certification after correcting identified deficiencies.
- Schedule the certification process with the accreditation agency.
- The Director of Information Services will attend/participate in the formal certification process.
- Plan future certification sessions on an annual basis.

INFORMATION SYSTEMS

It is the policy of CITY OF CALEXICO to evaluate all computer systems and corresponding networks to certify the level of security.

PROCEDURE:

- List the different computer systems within CITY OF CALEXICO.
- Conduct testing to evaluate the degree of security within each of the systems.
- Evaluate the outcome of the certification testing.
- Implement changes/alternations to ensure compliance with the certification security expectations.
- Conduct testing annually or according to the certifying/accreditation body.

MITIGATION

It is the policy of CITY OF CALEXICO to mitigate any harmful effects from the misuse of protected healthcare information by CITY OF CALEXICO or any business associates.

PROCEDURE:

- CITY OF CALEXICO is notified that confidential healthcare information has been misused by an employee or business associate.
- CITY OF CALEXICO shall communicate this information to the Privacy Officer.
- If the information has been misused by an employee, the policy on employee sanctions is to be implemented.
- If the information has been misused by a business associate, CITY OF CALEXICO is to:
    - Investigate the misuse of the information.
    - Determine if the misuse was serious.
    - Determine if the misuse is repeated.
    - Counsel the business associate on the misuse of confidential healthcare information.
    - Monitor the business associate's performance to ensure that the wrongful behavior has been remedied.
- CITY OF CALEXICO reserves the right to terminate a business associate agreement in the event the misuse of confidential healthcare information continues despite counseling.

SANCTIONS

It is the policy of CITY OF CALEXICO to apply sanctions to employees failing to comply with the policies and procedures regarding confidential healthcare information.

PROCEDURE:

- If an employee is found to violate any policy or procedure in regards to confidential healthcare information the CITY OF CALEXICO's policy on disciplinary action will be implemented.

- The severity of discipline will be determined according to:

    - The severity of the violation.

    - If the violation was intentional or unintentional.

    - If the violation indicates a pattern or practice of improper use or release of confidential healthcare information.

- The degree of discipline may range from a verbal warning to termination.

- Each episode of employee discipline regarding confidential healthcare information is to be documented and reported to the Privacy Officer.

- Documentation is to include:

    - Name of employee

    - Degree of violation

    - Location of violation

    - Date and time of violation

    - Disciplinary action provided

- Refer to CITY OF CALEXICO's Disciplinary Policy for further information.

COMPLAINT PROCESS

It is the policy of CITY OF CALEXICO to address any complaints with regards to protecting the privacy of confidential healthcare information.

PROCEDURE:

- Any complaint regarding the privacy of confidential healthcare information is to be made in writing to:

  City of Calexico
  ATTN: Privacy Officer
  1320 Sixth Street
  Orland, CA 95963
  (530) 865-1200

- Upon receiving the complaint, the Privacy Officer is to:
  - Document the complaint in the Complaint Log.
  - Document the date, time and name of person making the complaint in the Complaint Log.
  - Investigate the compliant.
  - Document the resolution of the complaint in the Complaint Log.
  - Communicate the outcome of the complaint with the individual filing the complaint.
- The Privacy Officer is to communicate the number of complaints and resolutions during routine executive level meetings of CITY OF CALEXICO.

SAFEGUARD OF CONFIDENTIAL INFORMATION

It is the policy of CITY OF CALEXICO to have sufficient safeguards in place to protect confidential healthcare information.

PROCEDURE:

- The following are to be used to protect confidential healthcare information:
    - Medical records of current patients on any patient care area are stored properly. The following employees are permitted access to these medical records:
        - Nurses
    - Individuals without permission to a patient's medical record are not provided access to the record.
    - Electronic/computerized records of any current or previous patient can only be accessed by those with permission to do so. Permission is granted via the log-in procedure and utilizing the designated password.
    - Any documents containing identifiable patient healthcare information are to be shredded prior to disposal.

PRIVACY TRAINING

- It is the policy of CITY OF CALEXICO to train all employees on the policies and procedures about confidential healthcare information.
    - The training must be appropriate for each level of employee to carry out their healthcare function within CITY OF CALEXICO.

PROCEDURE:

- Employees shall be categorized according to the degrees of access to confidential healthcare information.
- Inservice education programs are planned to address the degrees of access to confidential healthcare information.
- All existing staff are trained on the policies and procedures regarding confidential healthcare information.
- All future staff shall be trained during orientation on the policies and procedures about confidential healthcare information.
- The type, amount, date and employees who received training on the policies and procedures about confidential healthcare information is documented.

PRIVACY OFFICER

- It is the policy of CITY OF CALEXICO to employ one individual to serve as the Privacy Officer for the organization.
    - The Privacy Officer is responsible for ensuring the confidentiality of all patient confidential healthcare information.
    - The Privacy Officer is responsible for developing and implementing all policies and procedures effecting patient confidential healthcare information.
    - The Privacy Officer is responsible for limiting the incidental use of protected healthcare information.
    - The Privacy Officer is responsible for documenting, investigating and responding to all patient complaints regarding confidential healthcare information.

- CITY OF CALEXICO must provide the patient with the first request for a list in any 12-month period with no charge. CITY OF CALEXICO may charge the patient a reasonable, cost-based fee for each future request within the 12-month period provided that CITY OF CALEXICO informs the patient in advance of the fee and offers the patient the chance to withdraw or modify the request to avoid or reduce the fee.

- CITY OF CALEXICO must document the patient's request for a list, a copy of the information provided to the patient and the titles of the persons or offices responsible for receiving and processing the request by the patient.

ACCOUNTING OF RELEASED INFORMATION

- It is the policy of CITY OF CALEXICO to provide a patient with a list of times confidential healthcare information had been released over the last six (6) years.
    - CITY OF CALEXICO does not have to comply with this policy if the information was:
        - Used to provide patient care, payment for services or healthcare operations,
        - Provided to the patient,
        - Provided to employees responsible for the patient's care,
        - Accessed prior to the date of compliance to this policy.

PROCEDURE:

- A patient may request a list of times confidential healthcare information had been released over the last six (6) years.
- CITY OF CALEXICO is to provide a written account of the times this information had been released. This written account is to include:
    - The date of release.
    - Name of the person or entity and address who received the information.
    - A brief description of the information released.
    - A statement of the purpose for the information or, instead of a statement, a copy of the written request for the information.
    - If multiple requests were made by the same individual or entity, CITY OF CALEXICO is to provide the frequency, periodicity, number of times the information was released and the date of the last release during the period requested by the patient.
- CITY OF CALEXICO is to act on the patient's request no later than 60 days after receiving the request. CITY OF CALEXICO is to:
    - Provide the patient with the list.
    - Communicate to the patient the reasons why the list will not be prepared within 60 days.
    - Communicate to the patient the date in which the list will be prepared.
    - Complete the request within an additional 30 days.

PROVIDING A PATIENT WITH CONFIDENTIAL INFORMATION

It is the policy of CITY OF CALEXICO to provide a patient with confidential healthcare information upon request.

PROCEDURE:

- Any requests for confidential healthcare information by a patient are to be made in writing.

- The patient may request that the confidential healthcare information be sent to an alternative address if the patient can prove that the healthcare information could cause him/her harm. An alternative address is one that the patient feels is secure and that the information will not be inadvertently placed in someone's possession who could potentially cause the patient harm by having access to the information.

- CITY OF CALEXICO may place conditions on the request for confidential healthcare information. These conditions include:

    - Payment for providing a copy of the patient's confidential healthcare information.

    - The patient provides an alternative address or other method of contact.

- CITY OF CALEXICO does not require an explanation from the patient as to the reason why the patient wants a copy of their confidential healthcare information.

- CITY OF CALEXICO may refuse a patient's request if the patient has not provided information about payment.

REQUEST TO RESTRICT CONFIDENTIAL INFORMATION

It is the policy of CITY OF CALEXICO to accept a patient's request to restrict confidential healthcare information.

PROCEDURE:

- When a patient requests that CITY OF CALEXICO restrict the use of confidential healthcare information for treatment, payment or healthcare operations:
    - CITY OF CALEXICO does not have to agree with the patient's request.
- CITY OF CALEXICO may terminate an agreement to restrict the use of confidential healthcare information if:
    - The patient agrees or requests the agreement to be terminated in writing.
    - The patient agrees or requests the agreement to be terminated verbally and the termination is documented in the patient's medical record.
    - CITY OF CALEXICO informs the patient that the agreement to restrict confidential healthcare information is terminated. Information gathered during the terms of the restriction will continue to be restricted. Information gathered after the termination of the agreement will not be restricted.
- Evidence of agreements of restriction and the termination of such agreements must be made in the patient's medical record. This information is to be maintained by CITY OF CALEXICO for a period of six (6) years.

CONFIDENTIAL INFORMATION RELEASE

It is the policy of CITY OF CALEXICO to inform a patient of the uses, releases and patients' rights in respect to confidential healthcare information.

PROCEDURE:

- CITY OF CALEXICO has a privacy notice that states the patient's rights with respect to uses and releases of confidential healthcare information.
- CITY OF CALEXICO will provide the Privacy Notice to new enrollees at the time of enrollment.
- CITY OF CALEXICO will provide a copy of the Privacy Notice to any person upon request.
- CITY OF CALEXICO's Privacy Notice is posted on the web site.
- CITY OF CALEXICO will provide each patient with a copy of the Privacy Notice upon major revisions.
- CITY OF CALEXICO will retain a copy and any revisions of the Privacy Notice for six (6) years.

- Type of injury
- Date and time of treatment
- Date and time of death, if applicable, and
- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars and tattoos

- CITY OF CALEXICO is not permitted to release information about the patient's DNA, DNA analysis, dental records or samples, typing or analysis of body tissues or fluids.
- CITY OF CALEXICO prohibits the law enforcement agency from using the healthcare information for purposes other than the reason it was requested and requires the agency to return the information to CITY OF CALEXICO or destroy the information at the end of the litigation.
- CITY OF CALEXICO may release confidential healthcare information to a law enforcement official if there is evidence of criminal conduct on CITY OF CALEXICO's premises.
- CITY OF CALEXICO may release confidential healthcare information to comply with laws relating to workers' compensation or other similar programs that provide benefits for work-related injuries or illness.

- CITY OF CALEXICO will not inform a personal representative of the report of abuse, neglect or domestic violence if CITY OF CALEXICO believes the personal representative is responsible for the abuse, neglect or other injury.

- CITY OF CALEXICO may provide confidential healthcare information to a health oversight agency for the purpose of conducting audits, civil, administrative or criminal investigations, inspections, licensure, disciplinary actions or other activities necessary for the operations of CITY OF CALEXICO.

- CITY OF CALEXICO may not provide confidential information if the patient is under investigation or to investigate if the patient qualifies to receive public benefits when the patient's health status is needed to make the decision about receiving the public benefit.

- CITY OF CALEXICO shall provide confidential information in response to a court order. Only the information requested may be provided.

- CITY OF CALEXICO shall provide confidential information in response to a subpoena, discovery request or other lawful process.

- CITY OF CALEXICO may provide information to a law enforcement agency seeking confidential healthcare information if the agency has attempted to reach the patient using the patient's last known address, if the notice for the information explains the need for the healthcare information, and the time for the patient to raise objections to the law enforcement agency has elapsed.

- CITY OF CALEXICO may provide information to a law enforcement agency seeking confidential healthcare information CITY OF CALEXICO has attempted to reach the patient but was unsuccessful.

- CITY OF CALEXICO may provide information about certain types of wounds or other physical injuries upon court order, court-ordered warrant, subpoena, summons, grand jury subpoena, civil investigative demand or other similar process when it is determined that the information is relevant and material to the investigation and that de-identified information could not be used.

- CITY OF CALEXICO may provide confidential healthcare information to a law enforcement official for the purpose of identifying, locating a suspect, fugitive, material witness or missing person. This information is limited to:

    - Name and address

    - Date and place of birth

    - Social security number

PUBLIC HEALTH AUTHORITIES OR LAW ENFORCEMENT

It is the policy of CITY OF CALEXICO to provide patient healthcare information to public health authorities or law enforcement agencies without the written authorization of the patient or the opportunity for the patient to agree or object to the release of confidential healthcare information.

PROCEDURE:

- Inform the patient that confidential healthcare information may be provided to public health authorities. The content of the information may include:
    - Prevent or control a disease, injury or disability
    - Report a communicable disease
    - Report a birth
    - Report a death
    - Report child abuse or neglect
    - Report or collect information about adverse effects of food or dietary supplements
    - Report or collect information about defects or problems with a product including any deviations of a biologic product
    - Report defective products to enable product recalls, repairs, or replacements.
    - Follow up with the use of products to comply with the requirements of the Food and Drug Administration
    - Investigate a work-related illness or injury
- In the event that CITY OF CALEXICO believes a patient is a victim of abuse, neglect or domestic violence, protected healthcare information will be provided to a government authority, social service, protective services agency or other agency authorized by law to receive report of such abuse, neglect or domestic violence.
    - CITY OF CALEXICO will inform the patient if/when this information will be provided to report the abuse, neglect or domestic violence to an authorized agency.
    - The patient can refuse to have the abuse, neglect or domestic violence reported.
    - CITY OF CALEXICO can overrule the patient's decision to not report the abuse, neglect or domestic violence if it is determined that the reporting is necessary to prevent serious harm to the individual or other potential victims.

INVESTIGATION

It is the policy of CITY OF CALEXICO to investigate allegations of misconduct by a employee or business associate when confidential patient healthcare information is released as evidence of CITY OF CALEXICO's misconduct.

PROCEDURE:

- The employee or business associate must in all good faith believe that CITY OF CALEXICO has engaged in unlawful conduct, has violated professional standards, or the care, services or conditions provided by CITY OF CALEXICO potentially endangers one or more patients, employees or the public.

- The employee releases information to a health oversight agency, a public health authority, an accreditation organization or an attorney retained by the employee or business associate for the purpose of determining the legal options of the employee/business associate with regards to the conduct of CITY OF CALEXICO.

- In the event that an employee is a victim of a crime, CITY OF CALEXICO is not held responsible for the release of confidential healthcare information if the employee notifies a law enforcement official. The information provided by the employee must be:

    - About the suspected perpetrator of the criminal act.

    - The information is limited to:

        - Name and address

        - Date and place of birth

        - Social Security number

        - Blood type and rh factor

        - Type of injury

        - Date and time of treatment

        - Date and time of death, if applicable, and

        - A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars and tattoos

    - CITY OF CALEXICO may not release any patient healthcare information related to DNA, DNA analysis, dental records or samples, typing or analysis of body fluids or tissues.

PATIENT'S PERSONAL HEALTH CARE INFORMATION

It is the policy of CITY OF CALEXICO to provide patients with their personal healthcare information. This information can be provided through alternative means upon patient request.

PROCEDURE:

- In the event that a patient requests communication about their health information, ask the patient to place the request in writing. CITY OF CALEXICO does not need an explanation from the patient as to why the requested healthcare information is to be provided via an alternative means.

- Determine how the patient would like to receive this communication. Methods of communication include fax transmittal or postal mail.

- Obtain from the patient the mailing address or fax telephone number to send the information.

- Obtain from the patient any costs incurred to prepare and mail the requested healthcare information.

PATIENT'S PERSONAL REPRESENTATIVE

It is the policy of CITY OF CALEXICO to recognize a patient's personal representative as the patient with respect to the patient's private healthcare information.

PROCEDURE:

- Verify that the patient has another individual identified as a personal representative. This situation might exist in the case of an unemancipated minor.

- Recognize that a parent, guardian or other person acting in loco parentis has the authority to act on behalf of the patient who is an unemancipated minor. CITY OF CALEXICO shall rely on the representations provided on the CITY OF CALEXICO Enrollment Card to support the relationship.

- Realize that the unemancipated minor can over ride any decisions made by a parent, guardian or other person acting in loco parentis if he/she consents to the healthcare service. The minor's consent to healthcare will be acknowledged even if the parent, guardian or in loco parentis have not consented to the health service or if the decision for health service is in contradiction to the minor's decision. Document the decisions regarding consent to healthcare services provided to the unemancipated minor and the individual(s) responsible for the decisions.

- CITY OF CALEXICO may refuse to accept an individual as a personal representative of a patient if CITY OF CALEXICO believes the patient has been or may be subjected to domestic violence, abuse or neglect, or the patient's life could be endangered by the individual identified as the patient's personal representative.

- CITY OF CALEXICO may exercise professional judgment and decide that it is not in the best interest of the patient to accept the individual identified as the patient's personal representative should there be a threat of violence, abuse, neglect or endangerment of life.

BUSINESS ASSOCIATE

It is the policy of CITY OF CALEXICO to prevent the indiscriminate disclosure of individual patient healthcare information unless there is an agreement identifying the role of the business associate and the uses for the patient's healthcare information.

PROCEDURE:

CITY OF CALEXICO has business associate agreements in place with the following business associates:

Pinnacle Claims Management, Inc.

- CITY OF CALEXICO shall investigate compliance with the contract if a complaint is made that the business associate has violated the terms of the contract.

- CITY OF CALEXICO reserves the right to terminate the contract should it find that the business associate is in violation of any of the terms of the contract if steps to correct the breach fail.

- If after determining a business associate is in breach of contract and CITY OF CALEXICO finds it not feasible to terminate the contract, CITY OF CALEXICO shall notify the appropriate federal authorities to file the decision to maintain the services of the business associate.

VERIFICATION OF IDENTITY

It is the policy of CITY OF CALEXICO to verify the identity of any individual requesting access to confidential patient healthcare information.

PROCEDURE:

- Employees of CITY OF CALEXICO are to request identification from any person requesting confidential patient healthcare information if the identity or the authority of the person is not known to the employee.

- Employees of CITY OF CALEXICO are to obtain any documentation, statements or representations from the person requesting confidential healthcare information. The documentation, statements or representations can be either verbal or written. The decision to release confidential patient healthcare information can be made based upon written documentation if it is signed and dated by the individual making the request.

- CITY OF CALEXICO may rely on the following as verification of identity when the release of confidential healthcare information is being requested by a public official:

    - If the request is made in person, the person provides an ID badge, official credentials or other proof of status.

    - If the request is in writing, the letter is written on the appropriate government letterhead.

    - If the request is made by another person on behalf of a public official, a written statement on appropriate letterhead or other evidence or documentation such as a contract for services, memo or purchase order that establishes that the person is acting on behalf of the public official.

    - An oral statement of legal authority if a written statement would be impractical.

    - If the request is made in the form of a warrant, subpoena, order or other legal process issued by a grand jury or other judicial body.

AUTHORIZATION FORM

It is the policy of CITY OF CALEXICO to receive written authorization from a patient prior to releasing or utilizing healthcare information.

Authorization is always needed prior to releasing psychotherapy notes and prior to releasing confidential healthcare information for the purposes of marketing.

- Authorization is not needed if the notes are needed to carry out treatment, payment or healthcare operations by the originator of the notes.
- Authorization is not needed if CITY OF CALEXICO is using the notes for its own training programs in which students, or trainees learn under the supervision of CITY OF CALEXICO personnel.
- Authorization to use psychotherapy notes is not needed to defend a legal action or any other legal proceeding brought forth by the patient.

PROCEDURE:

- Determine if an authorization is needed from a patient to release confidential healthcare information. Authorization is always needed prior to releasing psychotherapy notes or for the purpose of marketing.
- Send the patient a CITY OF CALEXICO Authorization Form and review the purpose of the authorization with the patient.
- Ask the patient to read, complete, sign and date the authorization form on the designated areas. The patient shall be given a copy of the signed and dated authorization form.
- Authorization forms must be documented in the customer service notes, filmed and cross-referenced.
- CITY OF CALEXICO field offices are to fax the completed Authorization Form to CITY OF CALEXICO Customer Service.
- Place the completed authorization form with the patient's file. The Authorization form is valid for 24 months, or before, if indicated by the patient on the Authorization form.
- Explain to the patient that the authorization form can be revoked at any time. This revocation must be in writing using an CITY OF CALEXICO Authorization Revocation Form.
- CITY OF CALEXICO must retain the signed authorization form for a period of six (6) years.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

- It is the policy of CITY OF CALEXICO to use or disclose protected confidential healthcare information if:
    - The information is used to carry out treatment, payment or healthcare operations.
    - The information is used for treatment activities by a healthcare provider.
    - The information is used for a healthcare provider to receive payment.
    - The information is used for healthcare operations by a healthcare provider that has a relationship with the patient in an effort to detect healthcare fraud, detect abuse or compliance.

- Each written request for individual healthcare information by parties not directly involved in the provision of patient care is to be maintained by the CITY OF CALEXICO and retained for a period of six (6) years.

PRIVACY POLICY

The first-ever federal privacy standards to protect patients' medical records and other health information took effect on April 14, 2004 under the Health Insurance Portability and Accountability Act (HIPAA). Under these federal standards, CITY OF CALEXICO has developed the following HIPAA Policy and Procedure Manual.

It is the policy of CITY OF CALEXICO to protect the privacy of individual patient health information. Because of this, the amount of information accessible in response to a request for information is limited to the minimum amount needed to perform a specific type of work or to complete a function. Protected health information is information, including demographic data, that relates to the individual's past, present, or future physical or mental health or condition, the provision of health care to the individual, or the past present, or future payment for the provision of health care to the individual.

PROCEDURE:

- Reasons to provide individual patient health information include:
    - Treatment
    - Payment, or
    - Healthcare operations
- Individuals that have access to protected health information will provide individual healthcare information only for the following reasons:
    - Upon request of the patient.
    - If needed for healthcare treatment, payment, or healthcare operations.
    - If the request is made for the purpose of detecting healthcare fraud or abuse.
- Information provided for each request for healthcare information shall be limited to:
    - Complete legal name, address and telephone number
    - Date of birth
    - Social security number
    - Past medical history information
    - Documentation of completed diagnostic tests, laboratory values, results of procedures and surgical procedures
    - Claims status
    - Benefit information

City of Calexico

HIPAA Privacy Policy and Procedures Manual

Table of Contents