# ADMINISTRATIVE (A)

# POLICIES AND PROCEDURES

## SAN JUAN COUNTY PUBLIC HOSPITAL DISTRICT NO. 1

DBA SAN JUAN ISLAND EMS

DBA VILLAGE AT THE HARBOR

DBA VILLAGE AT HOME

APPROVED BY THE SAN JUAN COUNTY PUBLIC HOSPITAL DISTRICT #1 BOARD OF COMMISSIONERS ON 12/17/2025

# Contents

SAN JUAN COUNTY
Public Hospital District No. 1

# ADMINISTRATIVE POLICIES

## INTRODUCTION FOR ADMIN POLICIES AND PROCEDURES

### A.1 PREFACE

San Juan County Public Hospital District No. 1 operates the Village at the Harbor, Village at Home, and San Juan Island EMS. It has employees who may participate in either or both of these agencies, or neither.

As a result, the District has one set of binding Policies and Procedures for the entire district, as well as department-specific Policies and Procedures.

The date of the current version shall be used as the version number. Previous versions should be saved in accordance with retention schedules.

### A.2 DEFINITIONS

Please find below definitions of terms used throughout the document. Other, more specific terms and definitions will appear embedded in the document.

Agency / Division: A business unit within the public hospital district. Business units, such as Village at the Harbor, are considered "Agencies." The Administrative Division is the only division; its role is to support the Agencies and the Superintendent.

Agency Head: the Administrator for San Juan Island EMS, the Executive Director of Village at the Harbor, and the Executive Director of Village at Home, each leading an agency.

Commissioner; District Board: The Board of Commissioners of the San Juan County Public Hospital District No. 1, made up of five Commissioners; altogether, the District Board.

County: The auditing and financial management offices of San Juan County, Washington.

Department Head: Someone who runs a department within an agency. For instance, the Chef, who runs the kitchen, with the kitchen being the department.

District: San Juan County Public Hospital District No. 1, P. O. Box 370, Friday Harbor, WA 98250.

District Resolution: A resolution which has been duly voted on and approved by the District Board and signed by a minimum of four Commissioners of the District.

District Offices: The District operates four facilities in Friday Harbor, Washington: (1) Administrative Offices: 535 Market Street, Suite E; (2) San Juan Island EMS: Frank Wilson Memorial EMS Building,

1079 Spring Street; (3) Village at the Harbor: 543 Spring Street; and (4) Village at Home: 535 Market Street, Suite C.

Division: See "Agency/Division."

Employee: Generally, this refers to any person hired by the District, whether full-time, part-time, or volunteer. Where a more specific definition or meaning is intended, it is usually apparent from context or clearly stated, e.g., "full-time employee."

Section: A "Section" in these policies and procedures refers the entirety of a single policy and its procedures, e.g. "Payroll."

Senior Leadership / Agency Heads: This refers to the Superintendent, Deputy Superintendent, and Agency Heads.

Segment: A "segment" refers to an individual numbered portion of a policy

Treasurer: An official position designated by the Board to oversee the District's ledgers. This is a required step for a special-purpose taxing district to manage its own finances instead of the county's treasurer. On April 1, 2024, in accordance with Resolution 24-598, the Hospital District assumed control of its own accounts and created its own Treasurer in accordance with RCW 740.44.171.

Tyler Tech ERP Pro 10 / Tyler: The enterprise resource software the District uses to manage its general ledger. The District began using Tyler ERP Pro 10 on April 1, 2024, when it moved away from using San Juan County for general ledger management and installed its own Treasurer.

Tyler Pay: Tyler Payment Systems is the credit card processing module directly tied to the Tyler cashiering and general ledger systems. The credit card processing, payment management, and security protocols are managed and guaranteed by Chase Bank.

## A.3 PURPOSE, ADOPTION AND AMENDMENT OF POLICIES

### A.3.1 Purpose and Applicability

This Manual contains the San Juan County Public Hospital District No. 1's (the "District") policies and procedures. Policies may change as the District grows, laws and regulations change, or as needed to better serve the District residents and the District's personnel. The District, through appropriate deliberations of the District Board, reserves the right to modify, revoke, suspend, terminate or deviate from the policies set forth in this Manual at any time.

This manual includes all of the District's Policies and Procedures, which are separated into separate word/pdf files for ease of access, currently inclusive of Administrative, Personnel, Village at the Harbor, San Juan Island EMS, and Village at Home Policies and Procedures. These policies are intended to work harmoniously with each other and are all considered the District's policies.

While the District will try to provide advance notice of any policy changes, advance notice will not always be possible or practical. It is important to understand that these policies do not constitute an employment contract, or promises of specific treatment, or a promise of employment for any specific duration between the District and its employees.

This Policy Manual applies to all who do work on behalf of the District, such as employees of the District, volunteers, and commissioners. Some policies also apply to residents in the Village at the Harbor or other clients and members of the public that we serve. Specific policies or procedures may apply to a particular department (currently there are two agencies: Village at the Harbor and San Juan Island EMS), and will be clearly identified as such.

In cases where these policies conflict with a San Juan County ordinance, state or federal law, a valid and effective collective bargaining agreement (CBA), or an individual written employment contract, the terms of the law or contract shall prevail. Once approved, no Elected Official, supervisor, manager, or representative of the District, other than that arising from a duly authorized Resolution of the District Board, has the authority to make any written or verbal statements or representations that are inconsistent with these policies. The District sometimes uses employment agreements that deviate in small details, such as in regard to PTO accrual for a specific employee and may only be executed by the Superintendent or the Board of Commissioners.

For Federally-funded grant activities and expenses, if this policy conflicts with the requirements of 2 CFR part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, the stricter application of policy applies.

**A.3.2 Sources of Authority**

Legal and Regulatory Authority. It is the policy and practice of the District to comply with all laws and regulations in applicable jurisdictions. Many policies and procedures are written to ensure compliance with legal and regulatory requirements. Employees who are concerned about non-compliance should raise the issue with their supervisor rather than making unilateral decisions that differ from the District's Policies and Procedures.

"San Juan County ALS/BLS Protocols" are a source of Department of Health regulatory direction for San Juan Island EMS and should be treated as such. The most current version should be used.

Policies. The set of rules or guidelines for the organization and staff to follow in or to achieve compliance. They are the responsibility of the Board of Commissioners.

The District has "Bylaws" and a "Code of Ethics," that govern how the Board of Commissioners is run. These carry the weight of policy but are maintained separately from this manual. The Bylaws and Code of Ethics are updated by resolution of the Board of Commissioners.

Procedures. Procedures are instructions on how a policy is followed. They are the responsibility of the Superintendent and department heads.

Collective Bargaining Agreement (CBA). Union employees are subject to all Policies and Procedures, except where they differ in the CBA. The CBA shall always supersede a District Policy or Procedure. The CBA must be fully executed by the Board of Commissioners. Not all employees are members of a union, and the CBA only applies to valid members.

Standing Orders. These are operating guidelines or administrative directives in the form of written orders by the Agency Head, or as delegated by the Agency Head to department heads. These orders do not supersede formal Policies, but they may temporarily supersede a procedure, provided a

duration is clearly stated, and the person issuing the standing order has sufficient authority to do so – for instance, the Assistant Chief of San Juan Island EMS could not issue a standing order relating to Village at the Harbor operations.

Job Descriptions are an example of a standing order and must be approved by the Superintendent as they set pay ranges for employees as well as working conditions and requirements.

Verbal and Administrative Direction. Senior leadership and supervisors are authorized to give direction on a daily basis in the areas of their responsibilities and consistent with job descriptions. Just because something isn't written down, doesn't mean it isn't authoritative. However, these directions shouldn't conflict with these Policies and Procedures (see also A.4.2 Senior Leadership).

### A.3.3 Amendment of Policies and Procedures

Policies and any changes to those policies must be approved by the Board of Commissioners. It shall be the duty of the Superintendent to propose to the District Board of Commissioners any proposed modifications to these policies. Changes will be clearly marked, and the entire document passed in its entirety with the changes adopted collectively.

Procedures may be changed or added to by the Superintendent at any time (see below).

> Procedures for "Amendment of Policies and Procedures":
>
> Changes made to Procedures in this manual will be made in writing and clearly communicated to affected staff.

### A.3.4 Severability

If any provision of this title or its application to any person or circumstances are held invalid, the remainder of the title or the application of the provisions to other persons or circumstances is not affected.

### A.3.5 Creation of Forms

The District will manage the creation of forms to make implementation of these policies both practical and consistent across the district. These forms will be approved by the Superintendent. Forms specific to individual agencies may be approved by the respective agency head. All forms should comply with these Policies and Procedures.

## A.4 ROLE OF LEADERSHIP

### A.4.1 Board of Commissioners

The Board of Commissioners is responsible for ensuring that the District's Superintendent is performing to expectations. Part of that is monthly reports to the Board of Commissioners. This should include at a minimum:

- Monthly Operations Report
- Monthly/YTD P&L against Current Budget
- Basic Statistics (detailed stats are part of our QA/QI Process, which is not discoverable).
- Accounts Receivable Trending

- Other requested reports or work product, which is not discoverable.

Additionally, the Board is responsible for financial oversight (including budgets and monthly financial reviews) and must ratify all expenditure authorizations approved by the Agency Heads or the Superintendent.

The Board is further responsible for the overall vision and direction for the District. It is expected to rely on and/or include the Superintendent in this planning process, but is the sole prerogative of the Board of Commissioners to set this strategic direction.

**A.4.2 Senior Leadership**

The Superintendent shall direct the breakdown of these responsibilities among the management team and serve as the only linkage with the Board of Commissioners. The Superintendent may prepare resolutions for adoption as needed, and to be proposed to the Board, provided at least one commissioner is willing to support the resolution.

A.4.2 Procedures for "Senior Leadership"

Senior Leadership includes the Superintendent, Agency Heads, and assistant Agency Heads.

The role of the senior leadership is to give direction to staff and those we serve. They should:

- Assure the mission of the organization is followed.
- Provide a point of accountability.
- Establish clear position descriptions that direct the responsibilities and behaviors of staff. The organizational chart will define the chain of command for staff.
- Be accessible and responsive to staff and those we serve.
- Communicate the mission and philosophy with all staff and those we service.
- Be responsible for the financial well-being of the organization, including development of a fiscal plan.
- Advocate for and promote access to healthcare, including but not limited to assisted living, prehospital emergency care, and clinic and hospital services.
- Prepare and plan for service and care delivery

**A.4.3 Accountability Month**

It is the responsibility of both personnel and supervisors to ensure that these Policies and Procedures are followed. Management should ensure that an effort is made to be accountable to these Policies and Procedures, the law, and best practices.

Management may utilize "Accountability Month" as a way to help ensure that key compliance issues are addressed. This is voluntary, non-required way to improve outcomes within the hospital district. Failing to hold an accountability month in no way implies a failure to adhere to best practices, the law, and these Policies and Procedures.

## A.5 ACCESS TO PREMISES

Access varies based on use but is limited to those who have a need. Each facility has general access points that employees or the public may enter during business hours. Storage units for sensitive equipment or medications, records, staff offices, and other key locations require additional access via a keycode or locks.

Agency Heads set guidelines for access to their facilities through written or verbal direction.

Any employee issued any key to the District Offices will be responsible for that key during their tenure and/or association with the District. If the key is not returned upon leaving the District's employment, the employee or volunteer will be assessed a $200 fee. This will be deducted from the employee's last paycheck or billed to the employee or volunteer.

> Procedures for "Access to Premises"
>
> In all cases, Senior Leadership may have access to any space. Agency Heads determine who has access to which spaces.

## A.6 ACCOUNTING AND GENERAL LEDGER

### A.6.1 Responsibility for Financial Management

The Board of Commissioners must approve all budgets. It is the responsibility of the Superintendent to prepare and present those budgets to the Board of Commissioners and to ensure the District complies with all financial reporting requirements.

Other staff are expected to help support the budgeting process as requested. A monthly analysis of the district's finances will be submitted to the Board of Commissioners.

The Superintendent is responsible for the District's overall finances and operations. The Superintendent's authority may be delegated to Agency Heads by use a "Delegation of Powers" document or job description (and to a lesser degree the Assistant Administrator or Assistant Chief), which must be shared with the Board of Commissioners, and is attached to the job description. These policies and procedures also lay out rights and responsibilities of Agency Heads within the District.

The Board of Commissioners may opt to require changes to any delegated authority, but unless specifically stated otherwise, this authority rests with the Superintendent. The Board must set the delegated powers for the Superintendent in a similar manner, and the Delegated Powers for any other employee may not exceed these powers.

### A.6.2 Separation of Financial Process Preparation and Approvals

The Superintendent may authorize various employees to prepare warrants (accounts payable), deposits and/or billing (accounts receivable), payroll, and other financial processes such as monthly financial reconciliation. Those employees who prepare financial processes must not be the same as those approving these processes, that is, every financial process must have at minimum two designated people: the person(s) preparing and the person(s) approving.

On April 1, 2024, in accordance with Resolution 24-598, the Hospital District assumed control of its own accounts and created its own Treasurer in accordance with RCW 740.44.171. Resolution 24-598 furthermore established the position of Treasurer and Auditor for the District and assigned those roles to the Finance Director and Administrative Specialist of the District. The Treasurer and Auditing Officer are bonded for no less than $50,000 or equivalent insurance coverage to assure thefaithful discharge of their duties as part of the general liability coverage of the District.

Procedures for "Separation of Financial Process Preparation and Approvals"

**Preparation of financial processes for all agencies and divisions:**

- **Finance Department** prepares accounts payable, accounts receivable, manages and tracks deposits, performs monthly reconciliation, tracks budget, performs financial reporting, performs internal auditing, manages asset management, and performs other financial duties as required for all agencies.
- **Human Resources** prepares payroll, payroll-related accounts payable, and reporting for all agencies and departments.

**Approvers by agency:**

- **Hospital District Administrative Offices:** Hospital District Superintendent approves payroll, accounts payable, financial reporting, and other financial approvals as needed.
- **Village at the Harbor:** Executive Director approves all payroll, accounts receivable, and accounts payable within the limits set above.
- **Village at Home:** Executive Director approves all payroll, accounts receivable, and accounts payable within the limits set above.
- **San Juan Island EMS:** EMS Chief approves all payroll, accounts receivable, and accounts payable within the limits set above.

### A.6.3 Sources of Accounting Practices

On April 25, 2018, by Resolution 18-484 and with the approval of the Washington State Auditor's Office, the District changed its accounting to cash basis from the accrual/GAAP basis of accounting to align with the County's accounting system (Cash Basis).

The Hospital District uses the Budgeting, Accounting and Reporting System (BARS) of the Washington State Auditor's Office (SAO) to manage its chart of accounts, enabling the District to maintain a robust, easily searchable chart of accounts. Whether for tracking budgets, revenue, expenditure, or other metrics, reports on any number of criteria can be easily generated.

### A.6.4 Federal Grant Funds

Federal grant funds are skillfully accounted for using special project groups, which extend the BARS functionality even farther. Furthermore, all grant funds to date are direct cost funds. In the future, should the District enter into federal or other government grants wherein indirect costs are to be allocated, proper negotiations, rate proposals, and cost analyses will take place, and will require both the agreement of the District Board and the Grantor.

Funds drawn down from federal or state grant funds are strictly limited to those amounts needed to cover costs which are allowed under those funds. Funds from federal sources are to be drawn

down following the allocation of those funds as required to provide for the actual and immediate cash requirements of approved projects. Funds will not be drawn down to cover future expenditures.

On a monthly basis, after all invoice processing has taken place, the designated financial officer enters all expenditures into the Budget Tracking Worksheet for each award to ensure that the total costs do not exceed the amounts budgeted for the grant period. The Budget Tracking Report is then submitted to each of the Grant Project Directors and to the Superintendent for review. If significant variances occur, the variances will be documented, annotated and reported to the grant management specialists or other person as assigned to the specific grantor. If an updated budget is called for, the budget will be resubmitted for approval by the grantor.

For those grants which require matching, cost sharing (including cash and/or third party in-kind), those costs will be tracked using appropriate BARS codes in the Budget Tracking Report. This tracking will ensure that the funds or contributions are solely used for the purpose of the grant for which they are being tracked and are not included as contributions towards any other federally assisted project or program and are not being paid for by any other award or grant. Furthermore, every effort shall be given to show that the costs are actually necessary and reasonable for the proper and efficient accomplishment of the project or program objectives for the grant in which they are being tracked, and that they are for activities or costs that are allowable and provided for in the approved grant budget. As it relates to maintenance of effort, where applicable, Federal funds will supplement and not supplant current efforts and/or funding either from the District or from any other funding sources as specified in 45 CFR §75.306.

Any program income generated from any federal grant shall be allocated as set forth in the grant documents and shall be tracked both in the Budget Tracking Worksheet and monitored through the County accounting system. At present, the District grants do not foresee any program income, however, should income be generated the funds would be added and reinvested into the grant in order to help cover program costs.

### A.6.5 Financial Records Retention

As of April 1, 2024, the District's electronic financial records are securely stored in the cloud on its Tyler ERP Pro 10 system and are protected by robust cybersecurity protocols implemented by both Tyler Technology Inc. and the District's IT vendor, NW Technology Solutions LLC ("NW Tech"). All accounting data is retained electronically in the cloud, and the regular reports generated in the regular course of business are retained both electronically and in paper-filed format in the District Offices, as required. This source documentation includes, but is not limited to, records pertaining to the source and application of receipts and disbursements, federal awards, and income and interest. For more information on retention, please see A.22 Record Retention Policy.

### A.6.6 Investments

The District regularly invests excess proceeds in the Local Government Investment Pool (LGIP) when reasonable, under the direction of the Superintendent or the Finance Director and with clear communication between them. As this does not involve an actual expenditure of funds, it requires no special approvals except that it must be one of those two people. Sufficient funds should be held in the District Bank Accounts (see A.11 Bank Accounts) to cover its monthly bills.

### A.6.7 General Ledger Edits

In general, general ledger edits are minimal and should be managed by the Superintendent or the Finance Director at all times, with clear communication between them.

Procedures for "BARS Code Corrections and Creation of New BARS codes"

- In the event a deposit or expenditure is posted to the incorrect BARS code, a correction request will be made to the Finance Director.
- If a new BARS code is required, a request will be made to the Finance Director.
- New BARS codes and BARS code corrections must receive approval from the Superintendent, either verbally or through TylerTech. The GL Correction will be run in accordance with the appropriate procedures.

## A.7 ACCOUNTS PAYABLE AND CREDIT CARDS

### A.7.1 Accounts Payable

It is the District's policy to ensure that only approved invoices are paid, that payment is rendered only for goods and services actually received, and to ensure proper identification of expenses.

The Superintendent will ensure that the Board of Commissioners has the opportunity to review all financials and that it ratifies the authorizing officers' approvals through participation in the Board of Commissioners' financial committee meetings and Board meetings.

Procedures "Accounts Payable"

**Accountability and Receipts**

As set forth in section 6.2, all accounts payable must be approved by an Agency Head or the Superintendent (Authorizing Officer). The Authorizing Officer may utilize financial officers to prepare the payments for approval. All Agency Heads approving accounts payable shall ensure the following:

- Proof that a product or service was actually delivered, such as a packing slip, signed invoice, or affidavit, is submitted to the Finance Department by an employee who, in doing so, is verifying the products or services were rendered or received.
- Proof that products were actually delivered should be obtained and signed by someone other than the person placing the order, where possible.
- Billing statements are reviewed for accuracy by the Agency Head (i.e., to determine whether charges and credits from invoices or receipts are accurately reflected in the billing statement) before submitting to the Finance Department for payment.
- Each invoice to be paid is appropriately authorized.
- Every effort is made to ensure that all funds and accounts are internally managed and accounted for with precision.
- Blank checks are kept in a secure location and are accessible only to those who need them for their employment responsibilities.

**Process for Issuing Payments**

The following procedures shall be followed with accounts payable:

- When an invoice arrives, the Finance Department acknowledges receipt, files the invoice into the appropriate agency folder, and processes the invoice for payment according to the internal accounts payable cycle as regularly set by the District.
- Packing slips or receipts are initialed by those who received the goods, and they should not be the same person who placed the order. Upon receiving these packing slips, they are matched and attached to the applicable invoices.
- The Finance Department ensures that the correct BARS code for the entire invoice or separate line items, as applicable, has been applied. Agency Heads should review and approve the "cheat sheet" used to process payables. This will outline which BARS codes to use for everyday expenditures and will be cross-checked against the new year's budget before the start of the new year.
- If a vendor does not exist in Tyler, the Finance Department will request an up-to-date and signed W9 form and a Washington State UBI number from the vendor, and upon receipt, will create an active vendor account.
- If the Invoice is a timesheet or invoice related to a Federal or State grant, the Finance Department ensures:
    - the timesheet or invoice is signed by the appropriate manager and/or the Superintendent;
    - the amounts requested are in line with the budget;
    - enters the amounts into the respective spreadsheets;
    - all amounts and calculations balance appropriately;
    - the correct vendor code and BARS code are applied;
    - the worksheets and timesheets are then submitted to the Superintendent for approval; and
    - once approved, the appropriate funds are drawn down and/or requested from the relevant agency.
- In accordance with the District AP schedule, the Finance Department enters the invoices into Tyler and prepares an AP Payable packet.
- The Finance Department submits the AP Payable packet to the Agency Head for approval and/or the Superintendent, as applicable.
    - Agency Heads may authorize up to $5,000 per expenditure or routine expenditures that may exceed that number, provided they are recurring costs that are expected, routine, and anticipated.
    - The Superintendent may authorize any amount of expenditure and is responsible solely to the Board of Commissioners for complying with the approved budget.
    - Any unusual spending needs to be run by the Superintendent as soon as is feasible, especially when costs are uncertain, but Agency Heads are charged with the responsibility of dealing with emergencies responsibly, regardless of the availability of the Superintendent.
- Once approved by the authorizing Superintendent or Agency Head, the Finance Director performs a final accuracy and budget review and releases the AP Payable packet to be processed for payment.
- The Finance Department prepares the AP Payment packet and, upon authorization by the Finance Director, processes payment via check, EFT, or bank draft, as required.

- The Finance Department then files all the original signed invoices, receipts, reports, and lists electronically (in Tyler) and physically files the original paper copies according to the appropriate Document Retention Schedule in preparation for future auditing.
- At the end of the month, the Finance Department creates a monthly AP Check Register report for each District fund for that month.

**Note:** The Human Resources Manager will be solely responsible for processing payroll-related accounts payable, as payroll has already been reviewed and approved separately. Tyler may require an approval step, but there is no expectation that the Finance Director or Superintendent will perform this step.

**Review and Final Authorization of Accounts Payable**

- A day or two before the monthly Regular Board Meeting, the Board's commissioner delegate (usually referred to as the Board Financial Officer) attends the monthly financial meeting to review the monthly transactions, payroll, balances, reconciliations, and other financial matters as required by law and/or as further requested by the commissioner(s) (the Monthly Financial Meeting).
- The Board Financial Officer reviews and then provides approval by signing off on AP Monthly Check Register, the Monthly Payroll Reports, and the Monthly Financial Review.
- At the meeting of the Board of Commissioners, the board formally approves the monthly finances and expenditures, after which the Commissioners sign the Monthly Check Register and Monthly Payroll Report along with the other executable documents.
- If the Board of Commissioners disapproves of some claims, the Auditing Officer will recognize these claims as receivables of the District and will pursue collection diligently until the amounts are either collected or the Board of Commissioners approves the claims.
- Files are retained for a minimum of 6 years pursuant to the Washington State Secretary of State Core Retention Schedule DAN GS2011-184, Rev 3.

### A.7.2 Credit Cards

The District has a Visa credit card master account currently through Heritage Bank NW. The credit limit for the master account is set by the Board by resolution, and the various credit limits by card are managed by the Finance Director under the Superintendent's direction. Credit cards are issued to employees who have a legitimate, ongoing business need.

The cards are to be used for small and incidental office supplies, certain authorized travel and meal expenses, approved payments of online accounts, and for other expenditures as deemed necessary for the proper and smooth running of the various agencies of the District.

Any and all personal expenditures are strictly prohibited. Where accidental use of a District credit card for personal use occurs, repayment of funds to the District should take place within 30 days, and a copy of that repayment filed with the credit card payment record.

Credit Cards are a means of paying bills and are subject to the same approval as any other expenditure. Despite being issued a credit card, employees must still receive approval for

expenditures consistent with District policies and procedures. All credit card balances are paid in full every month.

Procedures for "Credit Cards"

**Accountability and Payment of Credit Cards:**

- Employees are responsible for all purchases made on the credit cards issued to them.
- At the end of the month, the financial officer sends the card statement and the Employee Credit Card Form to each cardholder along with the due date for return.
- Employee is responsible for reconciling all charges on the Employee Credit Card Form:
  - Receipts for all purchases must be attached.
  - Expenses listed in order of date of purchase.
  - The vendor, agency to charge, purpose of the charge, the amount, and the BARS code must be fully completed on the Employee Credit Card Form.
  - The total of the receipts and the form submitted must match the new monthly balance to be paid on the credit card.
- As with any expenditure, the employee's department head reviews and approves the Employee Credit Card Form and the invoice in accordance with section 7.1 Accounts Payable above.
- At the Monthly Financial Meeting, the Board Financial Officer checks the credit card transactions as part of his inspection.
- Any misuse of a District Credit Card will result in prompt action when instances of noncompliance are identified, including noncompliance identified in audit findings.
- Failure to comply with this policy can result in discipline (e.g., failure to collect receipts), typically progressive discipline, except in cases of deliberate misuse or particularly egregious instances.

**Request and Authorization for Agency Credits Cards**

The Finance Director will authorize credit cards for those with a legitimate need by request from Agency Heads or the Superintendent. The number of people having credit cards should be minimal.

Every credit card user will sign a Credit Card User Agreement, attesting to their responsibility for following these policies and procedures.

**Secondary Agency Credit Cards**

Agency Heads may also request a secondary credit card in their name for use by their staff to support the smooth operation of their business. Agency Heads are solely responsible for authorizing and managing the proper use and performing the monthly reconciliation of their secondary agency credit cards.

**Authorized Uses**

The Agency Head and the Finance Department are charged with the education of all authorized users of the credit cards regarding regulations and District policy for their use of the card(s).

- Only purchases of properly authorized items set forth by this policy for which funds have been approved in the agency's budget are allowed.
- All expenditures must be pre-approved by the appropriate Agency Head or Administrator. For employees who make regular, routine purchases (such as office supplies or medications), the Agency Head may authorize certain routine expenditures or authorize a purchasing cap.
- Under the general direction of the Agency Head, the financial officer tasked with accounts payable will develop a secure and accountable process for staff to (a) sign out agency cards not issued to a specific person and (b) to allow staff to request purchases.

**Travel**

Credit cards may be used for official business only. The District follows the current guidelines of the State of Washington Attorney General regarding eating and drinking at public expense. The Agency Head and/or Superintendent must pre-approve travel-related expenditures for overnight travel in accordance with current District policies on food and travel (see A.15 Expenditure Reimbursement: Meals, Awards, Travel, and Mileage Rules)

**Unauthorized Uses**

Cash advances on credit cards are prohibited.

Under no circumstances may any personal expenses be charged on District credit cards. Charges found not to comply with this policy are prohibited and will be the employee's responsibility. If, for any reason, disallowed charges are not repaid before the charge card billing is due and payable, the District shall have prior lien against and a right to withhold any and all funds payable or to become payable to the employee up to an amount of the disallowed charges and interest at the same rate as charged by the company which issued the charge card.

**Payment of Bills**

Credit card bills will be paid in full each month. To facilitate on-time payment of balances, the Superintendent will grant select personnel access to online credit card statements as needed.

**Use of Personal Credit Cards for District Business**

To ensure accountability for all District expenditures, employees should avoid using their personal credit cards to make purchases for official District business when possible.

However, the use of personal credit cards is acceptable for expenditures that have been appropriately authorized, and reimbursement may be requested, provided receipts and expenditures are fully accounted for in accordance with District policies.

### A.7.3 Other District Charge Accounts

The District also has charge accounts with various local and online vendors. A legitimate business need, with prior approval from the Agency Head, is required to use these accounts. Receipts, initialed by the authorizing Agency Head, must be submitted for every purchase, along with the appropriate BARS code and/or expense category.

Unauthorized use is subject to the same provisions of the credit card use policy above.

### A.7.4 Purchase Orders

Purchase Orders should be used for all expenses over $5,000 and should be signed by the Superintendent. The purchase order should be filed online in the Purchase Order folders and scanned into the appropriate AP packet in Tyler along with the invoice and packing slips. Public works and procurement policies should be followed as appropriate.

## A.8 ACCOUNTS RECEIVABLE AND DONATIONS

### A.8.1 Revenue Sources

The District maintains several sources for accounts receivable, such as:

- Assisted living fees – room, board, care, guest, concierge
- Home care fees – companion, personal care, housekeeping
- 911 EMS service fees – ambulance transport, GEMT
- EMS outreach programs – CPR/First Aid training, wilderness EMT, etc.
- Various grants – federal, state, regional, and local
- Donations

San Juan County collects property, leasehold, timber, and other taxes on behalf of the two Hospital District tax levies – the San Juan County Public Hospital District No. 1 Levy (the Primary Levy) and the San Juan Island Emergency Medical Service Levy (the EMS Levy). As a general practice, San Juan County will usually deposit the tax receipts for the two levies into their respective holding accounts around the 15th day of the following month in which the taxes were collected.

The District requires clear accounting for all revenues collected in its official course of business to ensure against theft or loss. While each agency has its own policies and procedures relating to fees and charges, the handling of revenues collected by the District should be in accordance with District policies and procedures as follows.

### A.8.2 Accounts Receivable

As of April 1, 2024, the Finance Director of the District became its Treasurer in accordance with RCW 70.44.171. The District maintains several accounts with Heritage Bank NW to manage the District's funds as follows:

- **Pooled General Ledger Account (5365):** The main account holding all funds of the Hospital District, which are tied to its General Ledger on Tyler.
- **6521 PHD Admin/Village at the Harbor/Village at Home Holding Account (5373):** Account used to hold deposited funds until they can be processed into the General Ledger.

- **6511 San Juan Island EMS Holding Account (5399):** Account used to hold deposited funds from Ambulance Fees and other sources until they can be processed into the General Ledger.
- **Credit Card and Online Processing Holding Account (5381):** Account used to hold credit card, e-checks, and other online payments processed through Tyler Pay until they can be processed into the General Ledger.

The District's holding accounts also provide additional security against cyberattacks and unauthorized transactions. To further protect against loss and fraud, the following policies govern the collection, deposit, and processing of funds:

- Cash or checks received by any agency must be held in a lockbox with sole limited access by the Finance Department and the Agency Head.
- A cash receipt will be written for all cash payments received and signed by the person accepting the funds.
- The original of the cash receipt will be provided to the payor, and a copy will be clipped to the cash, deposited into the agency's lockbox, and transmitted to the Finance Department along with the cash.
- All cash or checks must be transmitted to the Finance Department for processing within one business day.
- All funds must be deposited into the appropriate holding account within one business day of receipt of funds by the Finance Department and processed as accounts receivable into Tyler as outlined herein within seventy-two business hours.
- Credit card or e-check payments received through the online Tyler Pay portal will be transferred to the Pooled GL account and processed as accounts receivable into Tyler as soon as possible once the funds have cleared the Credit Card and Online Processing Holding Account.

Procedures for "Accounts Receivable"

**San Juan Island EMS – Ambulance Service Fees**

- Medical billing payments are primarily received by a 3rd Party Billing Company. These funds are deposited electronically into the San Juan Island EMS Holding Account.
- The 3rd Party Billing Company provides deposit receipts via email.
- On a weekly basis, the Finance Department matches the receipts provided by the 3rd Party Billing Company to the deposits actually received and reconciles the EMS Holding Account balance.
- All reconciled funds are deposited into the Pooled General Ledger Account and entered into the General Ledger by Journal Entry Deposit.
- Occasionally, San Juan Island EMS receives medical payments directly. Receipt of these funds are copied and sent to the 3rd Party Billing Company and processed as outlined above.

**San Juan Island EMS – Other Programs**

- EMS conducts a variety of fee-based classes. Contracted instructors and San Juan Island EMS staff may teach these classes.
- As a general rule, fees are collected as follows:
  - Classes organized by specific groups are invoiced.
  - Individual participants pay the instructor directly on the day of the class and are not invoiced.
  - At times, there may be a mixed class where one group is invoiced while the fees are paid directly by individual participants.
- The instructor of each class will complete the Training Center Fee Sheet for each participant and/or group and provide backup documentation for the class and/or qualification achieved by the participants.
- An individual receipt will be written for all cash received, and all cash and checks are deposited into the locked box as outlined in A.8.2 Accounts Receivable, above.
- All Training Center Fee Sheets are submitted to the Finance Department within 48 business hours of the class completion.
- The Finance Department prepares invoices for classes every two weeks.

**Village at the Harbor**

- The Agency Head, in coordination with the Finance Department, invoices residents for all rent and fees every month or as needed.
- These funds are deposited as outlined in A.8.2 Accounts Receivable, above.
- The Finance Department sends the Agency Head a weekly Aging History Report from Tyler to monitor past due accounts
- The Finance Department processes late fees after the invoice due date at the direction of the Agency Head.

**Village at Home**

- Due to the nature of their business and billing requirements, Village at Home directly invoices its clients in accordance with the Village at Home Policies and Procedures.
- The Agency Head provides the Finance Department with new client data as soon as it becomes available, who then creates accounts for each client in Tyler and returns the Tyler account number to the Agency Head.
- Agency Head sends invoices directly to clients and provides Finance Department with copies.
- The Finance Department enters the invoice information into Tyler, ensuring cash, check, and online Tyler Pay payments are processed seamlessly into the general ledger.

### A.8.3 Donations

The District complies with all applicable state and federal regulations governing the receipt of donations. The District is not a 501(c)(3) nonprofit organization, but as a municipality, donors may

make tax-deductible donations to the District. The District commits to treat all such donations with respect and appreciation.

In accordance with the A.8.2 Accounts Receivable, above, Donations are stored securely and processed promptly.

Procedures for "Donations"

Donations to a municipality are tax deductible for federal tax purposes and municipalities can issue a donation receipt for such donations. Title 26, Section 170(c)(1), of the Internal Revenue Code states that the term "charitable contribution" includes a contribution or gift to or for the use of a state or any political subdivision of a state if the contribution or gift is made for exclusively public purposes.

It is the donor's responsibility to request a receipt and provide an address (electronic or physical) to send the receipt. The District will provide to a donor the documentation needed to substantiate the gift for IRS purposes. This information can be found in IRS Publication No. 1771, Charitable Contributions – Substantiation and Disclosure Requirements, which is the basis for the following procedures.

Donors are responsible for obtaining a written acknowledgment from the District for any single contribution of $250 or more before the donors can claim a charitable contribution on their federal income tax returns.

The District does not accept donations for amounts under $250 or issue receipts for such donations. For donations of goods and services, consult the full IRS Publication.

**Written Acknowledgement**

Although it's a donor's responsibility to obtain a written acknowledgment, an organization can assist a donor by providing a timely, written statement containing:

- the name of organization
- the amount of cash contribution
- a description (but not the value) of non-cash contribution
- a statement that no goods or services were provided by the organization in return for the contribution, if that was the case
- a description and good faith estimate of the value of goods or services, if any, that an
- organization provided in return for the contribution

It isn't necessary to include either the donor's Social Security number or tax identification number on the acknowledgment. A separate acknowledgment may be provided for each single contribution of $250 or more, or one acknowledgment, such as an annual summary, may be used to substantiate several single contributions of $250 or more. There are no IRS forms for the acknowledgment. Letters, postcards, or generated forms with the above information are acceptable.

The hospital district shall generally send a letter to provide written acknowledgement.

### A.8.4 Online Credit Card and E-Check Payments

San Juan County Public Hospital District No. 1 accepts credit card and e-check payments for goods and services using its online portal with Tyler Pay. All credit card payment transactions comply with the Payment Card Industry Data Security Stand (PCI DDS).

Agencies that accept credit card payments are responsible for the appropriate transaction, documentation, and reporting procedures associated with this policy.

This policy applies to all Hospital District employees who accept credit card payment for goods, services, or donations.

Procedures for "Online Credit Card and E-Check Payments"

**General**

Credit card and e-check payments are accepted through the Tyler Pay online portal, accessible at sjcphd1.org/payment-portal. Payments can be accepted for invoices processed through Accounts Receivable or for other miscellaneous payments, including donations.

The Finance Department will create and update online payment guides.

Employees may assist clients with the payment process, but clients are solely responsible for accessing the online portal and initiating and authorizing payment. Employees may not write down or otherwise copy or retain a client's card or payment information.

If a question arises and the client needs further assistance, they should be referred to the Finance Department, located in the Administrative Office at 535 Market Street, Suite E. The Finance Department has a physical credit card processing device and accepts payments by phone or in person during regular business hours.

**Processing Fees**

A processing fee will be added to each transaction to cover the actual costs the District incurs from the bank, as detailed below:

- **Credit card payments:** 3.75% of the total transaction or a minimum of $2.50. (For example, a $1,000 transaction will incur a fee of $37.50, which will be added to the total transaction.)
- **E-check payments:** $1.95 flat fee per transaction. A $35 fee will be charged for each returned transaction.

**Payments from Invoice**

Village at the Harbor, Village at Home, and EMS residents and clients who have been provided an invoice may pay their outstanding invoices via the Tyler Pay online portal by clicking "*Pay Your Invoice Here*" under "*Available Services*."

**Miscellaneous Fees**

For class individual class charges or other fees such as guest meals for which there is no invoice, clients may make payments on the Tyler pay online portal by clicking "*Miscellaneous Payments*" under "*Available Services*."

## A.9 ANNUAL AUDITS

As a public entity, the District expects to be audited regularly by the State of Washington but must be audited at least once in three years by state law. There are three kinds of audits: (1) Accountability, (2) Financial Statements, and (3) Single Audits. It is the Superintendent's responsibility to ensure compliance with audits, typically by assigning responsibility to employees and reviewing the work before submission.

An accountability audit evaluates whether the District has adhered to applicable state laws, regulations and its own policies and procedures. The state audits these records to ensure public funds are accounted for and controls are in place to protect public resources from misappropriation and misuse.

The state performs financial statement audits of the District to provide an independent opinion on the District's financial statements and the results of its operations and cash flows. In other words, these audits determine whether the financial statements present a reliable, accurate picture of a government's finances. Financial audits are required for any local government in the State of Washington which receives over $2 million in annual revenues, or spends more than $750,000 in federal financial assistance, or is specified in financing arrangements, such as bonds, loans or grant agreements.

Lastly, the District is required to prepare the Schedule of Expenditures of Federal Awards (SEFA) to determine if an audit is required to be performed in accordance with the Single Audit Act for fiscal years (FY) with expenditures of federal awards of $750,000 or more. If this is required, the District shall use the State Auditor's Office for that audit, and reports on these audits will be submitted to the Federal Audit Clearinghouse (see 45 CFR 2 §75.501) within the earlier of 30 calendar days after receipt or nine months after the FY's end. Recipients must submit audit reports and appropriate forms to the FAC electronically at https://harvester.census.gov/facides/account/login.asp.

The District is also required by RCW 43.09.230 to submit an annual financial report to the State Auditor's Office within 150 days of the end of its fiscal year. The District will fully comply with the State auditor's office in all instances, and fully support the audit process, meeting all deadlines set by the State of Washington and the Federal Government. Any deficiencies will be fully addressed and an action plan for improvement implemented.

## A.10 ASSETS

### A.10.1 District Assets

All assets, whether fixed assets, small equipment, small and attractive assets, or supplies which have been purchased using District funds are the property of the District (District Assets) and have been purchased with taxpayer money.

As such, employees of the District and those working in the District offices under federal and/or other grants are expected to use and maintain all supplies and equipment in a conservative manner. All excessive or unnecessary use of water, electricity, medical supplies, office supplies, and equipment must be avoided.

### A.10.2 Purchasing and Preventing Theft

It is the responsibility of the Agency Head to execute the budget for routine expenditures within the constraints set by the Superintendent and in accordance with the Agency Head's delegated powers document. It is also the Superintendent's responsibility to implement procedures that ensure accountability.

Employees shall not accept any gift or other compensation from a supplier other than pads, pencils, and similar small items.

Procedures for "Purchasing and Preventing Theft"

**Asset Management**

While asset management is primarily focused on goods with significant value, it is important to ensure that smaller items, such as office supplies, batteries, etc., are not appropriated inappropriately for personal use. The purchase of office supplies must be approved by the Agency Head, but the actual purchasing may be done by a financial officer delegate.

**Delegation of Powers**

- Any non-routine expenditure must be authorized by the Superintendent (i.e. not an expense that can be expected every month or on a regular basis/schedule)
- All expenditures must be approved by the Agency Head and made consistent with expectations set by the Superintendent
- The purchase of any item over $5,000 requires approval from the Superintendent.
- No expenditure may be made that is not in the budget unless there is a motion or resolution of the Board of Commissioners

Someone different from the person ordering items should verify receipt of goods on packing slips to ensure no diversion of goods or services (see A.7.1 Accounts Payable). Supplies should be monitored by administrative staff to ensure that items are not inappropriately diverted.

Every effort will be made to manage costs by searching the internet, reputable contractors/sellers and all available sources to find the most reasonable for a product without surrendering quality and durability to provide the best value for money to our taxpayers.

**Consumables**

The District purchases and makes use of a number of consumable goods, from food for Village at the Harbor residents to medications and office supplies. Consumables should be kept in a secure location where possible and accessed only by those who have a need. This

is problematic with things like office supplies, but supply levels should be monitored for unexplained excessive use.

**Consumables – EMS Medications**

The District follows the Medical Program Director's policy on medication and equipment storage, substantially reproduced here.

- Medications and medical goods, when a printed expiration date is present, shall not be placed on a response vehicle or used on a patient, when that expiration date has passed.
- All expired medications and goods, once expired, will be taken off of the response unit and destroyed or used exclusively for training purposes.
- Destruction of controlled substances will follow the applicable county controlled substance policy (19-03) set by the Medical Program Director.
- All response units are subject to random and scheduled inspections by the Medical Program Director as well as the Washington State Department of Health, Office of EMS.
- Exceptions may be made when items are unable to be obtained through usual means. These exceptions may only be granted by the Medical Program Director in consultation with the manufacturer and will display a revised expiration date.

**References:**

- RCW 18.73.145
- WAC 246-976-300
- WAC 246-976-340
- WAC 246-976-390
- WAC 246-976-920

### A.10.3 Purchases of Small and Attractive Assets

For the purchase of all Small and Attractive Assets and Capital Assets which does not cost more than the Federal Simplified Acquisition Threshold (see 45 CFR §75.329), every effort will be made to purchase said items by checking the WA Current Contracts Portal, and also ensuring that said provider/seller does not appear on the Excluded Parties List System, within the Federal System for Award Management ("SAM") (a "SAM Excluded Party").

Agency Heads must authorize the purchases of small and attractive assets, subject to constraints as laid out above. It is the responsibility of management to:

- Estimate the annual expenditure for each supply item.
- Assess the availability of storage and the possibility of spoilage.
- Monitor all supply acquisitions.
- Minimize duplication of orders and other problems.
- Review supplier bills.
- Look for potential over utilization of individual items.
- Maintain an inventory of all District office supplies.

### A.10.4 Small and Attractive Assets ($300 - $5,000)

Assets and equipment costing $300 to $5,000 each are considered small and attractive assets ("Small Attractive Assets"). Specific items of interest are laptops and notebook computers, tablets, smart phones, conference sound and video equipment, and other similar assets. These assets should be responsibly tracked, and surplused in accordance with state guidelines.

Procedures for "Small and Attractive Assets"

When the District acquires Small Attractive Assets:

- Every Small Attractive Asset is tagged with an inventory number and is recorded in the agency asset tracking software or spreadsheet.
- The list of assets tracks the purchase date, inventory number, source of funding, location, and condition of the asset. This list is hand-inventoried on an annual basis by administration and is submitted to the Superintendent for approval.
- When a Small Attractive Asset has depreciated, worn out, or otherwise ceased to function and cannot be repaired (Surplus Small Attractive Asset), it shall be disposed of in a safe, standardized, and documented manner, in compliance with Washington State Auditing requirements. If the item is still operating but is obsolete for the purposes of the District, the Surplus Small Attractive Asset will be properly valued by someone with professional knowledge of items of its type. It is then disposed of in a documented manner with at least two District employees present to witness its disposal.
- A signed Affidavit of Disposal will accompany the District Resolution declaring the asset surplus. At least annually, the Superintendent will prepare a Resolution to be brought before the Board, listing the items and the manner of lawful surplus. Upon District Board approval, the surplus will be noted in the Small Attractive Asset management program, and the accountant will be notified to ensure proper accounting within the appropriate budgets and reports.

### A.10.5 Capital Assets ($5,000+)

District Assets with an appraised value over $5,000 are considered capital assets ("Capital Assets"). This may include but is not limited to:

- Vehicles
- Certain Communications Equipment
- Certain Medical Equipment
- Large Fixtures and Furniture
- Building and Facilities
- Large Training Equipment
- Other non-disposable items over $5,000 in value.

Procedures for "Capital Assets"

See also A.7.4 Purchase Orders

When the District acquires Capital Assets:

- Every Capital Asset is tagged with an inventory number

- The Capital Asset is then entered into the asset management system, thus tracking the purchase date, inventory number, source of funding, location, condition of the property, and current market value.
- Each year, the list is to be hand-inventoried and witnessed by the Agency Head
- When a Capital Asset has depreciated, worn out, or otherwise ceased to function and cannot be repaired ("Surplus Capital Asset"), it shall be disposed of in a safe, standardized, and documented manner, in compliance with Washington State Auditing requirements. The Surplus Capital Asset will be properly valued by someone with professional knowledge of items of its type. It is then disposed of in a documented manner with at least two District employees present to witness its disposal. A signed Affidavit of Disposal will accompany the District Resolution declaring the asset surplus.
- On at least an annual basis the Superintendent will prepare a Resolution to be brought before the Board, listing the items and manner of lawful surplus. Upon approval by the District Board, it will be noted in the Capital Asset management program as to the surplus and the accountant will be notified for proper accounting within budgets and reports if it was considered a capital expense.
- If the asset item is usable but obsolete for the purposes of the District, upon approval by the District Board, it may be advertised for sale to the public and sold for its established value. Written documentation will be provided for review by the District accounting firm and Washington State Auditors.

**A.10.6 Federally Acquired Assets**

As set forth in 45 CFR § 75.319-20, all assets purchased under a Federal award will be held under conditional title by the District, unless otherwise stated in the Federal Award ("Federal Assets"). Items costing more than the Federal Simplified Acquisition Threshold (see 45 CFR §75.329) will be made to purchase said items by checking Washington State Department of Enterprise Services Current Contracts portal ("Current Contracts Portal"), and also ensuring that said provider/seller is not a SAM Excluded Party.

Every effort shall be made to provide for the open, fair and transparent competition for any requests for proposals for work or the acquisition of assets.

Procedures for "Federally Acquired Assets"

As with the District Assets, Federal Assets will be assigned a company asset number, tagged, and accounted for in a computer-based control system and coded as Federal Assets. The District accounting firm shall track Federal Assets for the purchase date, inventory number, source of funding, location, condition of the property and its specific depreciated financial value.

All assets procured with Federal funds shall be protected, locked and/or stored in the District Offices when not in use for the purposes and for the grant for which they have been acquired. For equipment to be used off-site, the equipment must remain in the possession of or reasonably near those who have been authorized to use the equipment, as appropriate in the normal course of their duties.

When Federal Assets are no longer needed, wear down or become obsolete (Federal Surplus Assets), the District shall declare the property excess to the Federal awarding

agency and seek their instruction as to the disposition of the Federal Surplus Asset. Notwithstanding 45 CFR § 75.319, if the District has not received instruction from the Federal agency within 120 days the District shall dispose of the equipment as follows:

- Small Attractive Assets may be retained, sold or otherwise disposed of by the District with no further obligation to the Federal awarding agency.
- Unless otherwise instructed, Small Attractive Assets per-unit fair-market value more than $5,000 may be retained by the District, transferred back to the Federal Government, transferred to an eligible third party for use in a Federally-, State- or County-approved program or sold.
- If the District is authorized to sell the Capital Asset, the District's valuation and sales procedures shall be followed.

## A.11 BANKING

### A.11.1 Accounts Held

The District has multiple bank accounts with Heritage Bank as follows (see also A.8.2 Accounts Receivable):

- **Pooled General Ledger Account (5365):** The main account holding all funds of the Hospital District, which are tied to its General Ledger on Tyler.
- **6521 PHD Admin/Village at the Harbor/Village at Home Holding Account (5373):** Account used to hold deposited funds until they can be processed into the General Ledger.
- **6511 San Juan Island EMS Holding Account (5399):** Account used to hold deposited funds from Ambulance Fees and other sources until they can be processed into the General Ledger.
- **Credit Card and Online Processing Holding Account (5381):** Account used to hold credit card, e-checks, and other online payments processed through Tyler Pay until they can be processed into the General Ledger.

Collectively, the "District Bank Accounts."

The District also maintains an investment account with the Local Government Investment Pool managed by the Washington State Treasurer as mentioned in section A.6.6 Investments, above.

### A.11.2 Access to Bank Accounts

Access to the District Bank Accounts is approved by the Board of Commissioners and managed by the Superintendent to ensure that only necessary access is granted and that funds remain accountable and secure. Access is set by Board resolution and updated annually (or more frequently, as needed).

The Superintendent, another senior employee the Superintendent chooses (usually the Deputy Superintendent), the District Treasurer, and two members of the Board (typically the Board's financial officer and the Chair of the Board) are signatories on the accounts.

Checks are issued by the Treasurer from the Pooled General Ledger Account to make payments authorized by the Agency Heads and/or the Superintendent (see A.7.1 Accounts Payable). All checks require two signatures, generally the Treasurer and the Superintendent.

From time to time, checks must be drawn from one of the holding accounts and require two signatures as outlined in section 7.1 Accounts Payable, above.

There is no signature requirement to transfer funds between holding accounts and the General Ledger Account; however, all fund transfers between accounts must be processed by the Treasurer and/or the Superintendent.

The District has established electronic access to view transactions and download statements. This is set by the Superintendent and the Treasurer as needed operationally.

Upon the electronic receipt of drawn-down funds from a federal, state, or private grantor into the respective holding account, the Treasurer will transfer the funds within one business day to the General Ledger Account and apply said funds into the appropriate budget account as revenues to cover the amounts that have already been paid from the District's general fund for said grant.

### A.11.3 Additional Protections from Theft

As outlined previously, the person(s) preparing accounts payable for disbursement should not be a signer on any bank accounts. This prevents a single person from both issuing and authorizing checks, thereby making it easier to divert a purchase.

However, access to account information may be authorized at the Superintendent's discretion.

## A.12 CAPITAL IMPROVEMENT AND PUBLIC WORKS

### A.12.1 Contracting

In the course of its daily operations, the District employs a variety of contractors. The District first determines whether it is able to perform the functions using its in-house staff; and if not, will seek assistance. The District will also look into whether the functions the District is proposing are currently performed by bargaining unit employees or may fall within the scope of the bargaining unit. These services include but are not limited to, accountants, advisors, auditors, lawyers, information technology, help desk and security monitoring firms, secure shredding services, and web design, among others.

Procedures for "Contracting"

As a hospital district, there is generally no legal requirement to engage in a "Request for Proposal" or competitive bidding process for personal services. Additionally, due to the rural and isolated nature of island living, options may be limited in any case. However, there are many requirements regarding public works, procurement, and prevailing wages.

Service providers are hired based on their experience, history, ability to provide effective and timely service to our rural island, and reasonable costs and fees for services. Furthermore, every effort shall be made to provide for the open, fair and transparent competition for any requests for proposals for work or the acquisition of assets. The District also works with these providers to ensure that procurement processes, where applicable meet county, state, and federal guidelines.

Procurement of equipment or subcontracted services by our existing consultants and contractors must likewise check the party is not a SAM Excluded Party, and the Current Contracts Portal in order to ensure the District is getting the best value for money and efficient service for our taxpayers. Furthermore, contractors that help the District develop or draft grant applications, or contract specifications, requirements, statements of work, invitations for bids and/or requests for proposals, will be excluded from competing for such procurements.

### A.12.2 Design Services

The District is obligated by state law to engage in a "Request for Qualifications" or "Request for Proposals" process when engaging architectural, engineering, land surveying, and landscape architecture services.

### A.12.3 Construction Contracts

The District is committed to following all state and regulatory requirements for new construction projects, which should be thoroughly reviewed with the District's legal counsel before undertaking any such projects.

### A.12.4 Architectural & Engineering and Services

Architectural and engineering services are defined as follows:

- Architecture
- Engineering
- Land surveying
- Landscape architecture

Procedure for "Architectural & Engineering and Services"

**Project Bidding**

For specific services the District will public a Request for Proposals. All responsible bidders will be invited to submit a bid.

For general services, on a contracted and recurring basis, the District will publish a Request for Qualifications. All responsible bidders will be invited to submit their qualifications for consideration.

**Firm/Business Selection**

Selection of a firm or business for any architectural or engineering project will be based on qualifications, not the lowest bid. It is the responsibility of the District to ensure that the following conditions are considered for each bidder, regardless of the cost of their bid:

- Expertise
- Qualifications
- Previous projects and outcomes

The most qualified firm/business, determined through a preset list of qualifications, will be awarded the project.

**Contracting**

All firms/businesses that work with the District on architectural or engineering projects are required to sign a contract, outlining at minimum the following conditions:

- The scope and estimated total cost of the project.
- Agreement to adhere to all laws and regulations outlines in RCW 39 regarding architectural and engineering services provided to public agencies.
- District ownership of any materials, such as blueprints, presentations, charts, etc. produced specifically for the project by the firm/business.
- Right to terminate contract.

Contracts will be created by legal counsel and presented to the firm/business for review at the District's discretion.

### A.12.5 Professional Services

Professional and Purchased services can be defined as skills that cannot be classified as architectural or engineering and are predominantly intellectual in nature.

Purchased services can be defined as routine, repetitive, or mechanical in nature, that generally follow an established or generalized procedure and involve minimal levels of decision making. Purchased services comply with the prevailing wage laws established in 39.12. For District Policies and procedures related to prevailing wage, please reference A.12.8 Prevailing Wages.

Professional and purchased will be contracted, at the District's discretion.

### A.12.6 Material Acquisition & Purchasing

Material Acquisition and Purchasing can be defined as the purchase of materials not directly associated with a public works project. Materials purchased in correlation or solely for a public works project must follow all regulations regarding the public works bidding process, located under section A.12.7 Public Works. Material acquisition and purchasing does not apply to vehicles, equipment, or supplies.

Procedure for "Material Acquisition & Purchasing"

**Purchases of $75,000 or Less**

For purchases of $75,000 or less no competitive bidding is required. The Hospital District may contact vendors directly seeking a quote, there are no minimum quote requirements.

*Note: Dividing a project into multiple parts to remain under the $75,000 purchase maximum to avoid the bidding process does not circumnavigate the laws. The **total cost** of the project must be used to determine whether the project requires competitive bidding.*

**Purchases of More Than $75,000**

For purchases exceeding $75,000, the District must comply with all bidding laws set forth in RCW 39.26, the "Procurement of Goods and Services". The District will undergo competitive bidding for the purchase of the stated materials. The Hospital District will publish a press release in all local newspapers with a description of the requested materials and invite any vendors to submit

a bid at least 13 days prior to the submittal deadline. Additionally, the Hospital District holds the right to reach out to contractors and invite them to bid on any project.

The press release will include, at minimum, the following information:

- A detailed explanation of the required equipment, material, or supplies.
- An explanation of public works projects and a disclaimer regarding material acquisition and purchasing.
- Individual to contact for further information on the request.
- Where to submit bids and the name of the Public Works Project Coordinator.

For any vendor's bid to be considered, they must be regarded as a "responsive bidder" by meeting the following conditions:

- A 5% bid guarantee is required. A bid guarantee is a monetary deposit or bond that contractors must submit along with their bids to provide assurance to the District that they have the necessary funding to successfully complete the project.
- Have a valid unified business number (UBI).
- Have applicable experience manufacturing the products requested by the District, and upon request, be able to provide a portfolio of previous and successful large-scale projects of similar size and value.
- Within the three-year period immediately preceding the date of the bid solicitation, not have been determined by a final and binding citation and notice of assessment issued by the Department of Labor and Industries or through a civil judgment entered by a court of limited or general jurisdiction to have willfully violated, as defined in RCW 49.48.082, any provision of chapter 49.46, 49.48, or 49.52 RCW.

The project will be awarded based off one of the following determinations. The Superintendent is responsible for deciding which factor will be considered most important, based off the known information regarding the project. Only one of the following options may be used to determine bidder selection:

- Bids may be reviewed and awarded to the lowest responsive bidder.
- Bids may be reviewed and awarded to the most qualified and experienced bidder. Qualification and experience will be determined based on the plans and specifications submitted with the vendor's bid.

**Brand Name Specifications**

The Hospital District may specify a brand in the invitation to bid on a product if the Board, or their designated official, have determined that a certain brand name is of higher quality or better suited to the municipality's needs.

**Competitive Bidding Exemptions**

In some instances, the District is exempt from the competitive bidding process when a project is over $75,000.

- Emergency purchases: when a real or imminent threat is presented to the District, the District may forgo the competitive bidding process for material acquisition and select the vendor that can provide services to the District in the quickest fashion.
- Sole source purchases: when a product is only available from a singular vendor or limited due to geographical constraints, the District may forgo the bidding process. The District must be able to provide evidence and documentation that show lack of competition in the market. Additionally, the District must be able to provide research that shows that the cost for the product is still fair and reasonable. Examples of sole source purchases include:
- Patented products
- The purchase of equipment that must be compatible with existing equipment.
- Purchases involving special facilities or market conditions: If the Hospital District can secure equipment at a significantly discounted rate, the bidding may be waived for the project. Examples include:
- Auctions
- Going out of business sale
- The purchase of used equipment at an exceptional rate
- Purchases of insurance or bonds

**Piggybacking**

Piggybacking refers to the process of a public agency using another public agency's procurement contract for products and services to meet their own needs. Piggybacking can only occur when the soliciting public agency includes the option for other agencies to access the solicited materials in the contract.

When piggybacking occurs, the public agency joining the contract may waive the bidding laws set forth in RCW 39.26.

The District may "piggyback" on another public agency's public procurement contract when the following conditions are met:

- The host must be a public agency.
- The District must have a cooperative purchasing agreement with the Host.
- The Host must comply with their own bidding requirements.
- The Host must post the bid on the web.
- The Invitation to bid must state that the proposed contract can be used by more than one public agency.

### A.12.7 Public Works

Public Works, according to RCW 39.04.010, are defined as, "all work, construction, alteration, repair, or improvement executed at the cost of the state or of any municipality".

Examples of projects that would classify as public works include, but are not limited to, the following examples:

- Painting
- Installing new flooring

- Fixing a broken toilet
- Installing a retaining wall
- Janitorial services
- Remodeling a kitchen or bathroom
- Building construction
- Repaving a parking lot
- Upgrading an HVAC system
- Installing new lighting

Procedure for "Public Works"

**Project Planning and Approvals**

All projects involving outside contractors or laborers through the Hospital District must complete Public Works Flow Chart to determine whether their project classifies as "Public Works".

Prior to the commencement of any Public works Project, Agency Heads/administrators must complete the Public Works Approval Formand obtain the necessary signatures. All public works projects exceeding the Agency Head's spending authority must receive approval on the Public Works Approval Form from the Superintendent.

The Public Works Project Coordinator will ensure compliance on all public works projects. The Public Works Project Coordinator will be a position designated to one District employee by the Superintendent. The Public Works Project Coordinator will be responsible for managing and facilitating the Bidding, Contracting, Bonding, and Prevailing Wage aspects of any public works project. They will be expected to work within the guidelines set by the Superintendent and/or Administrator on any designated projects. The Public Works Coordinator must review and sign all Public Works Approval Forms prior to commencement of work to verify compliance with all laws and regulations in RCW 39 to the best of their knowledge.

**Bidding**

| | |
|---|---|
| **Formal Bidding Process** | **$350,000 +**<br>The District will publish a press release in all local newspapers. The lowest responsible bidder will be selected for the contract. |
| **Small Works Bidding Process** | **$0-350,000**<br>The District will use MRSC's Small Works Roster to request bids from listed contractors.<br>For projects ranging from $0-75,000 the most suitable contractor for the job will be selected from MRSC's Small Works Roster. For projects ranging from $75,000-350,000, a |

| | |
|---|---|
| | minimum of five bids will be obtained from MRSC's Small Works Roster. |
| **Emergency Work** | **No Range**<br><br>Emergency work will meet the definitions set forth in the policy as well as the laws and regulations outline in RCW 39. No bids are required for emergency work. |

**Formal Bidding Process**

The Hospital District observes all bidding laws and regulations set forth in RCW 39.

For projects totaling more than $350,000, the Hospital District will undergo competitive bidding for the project. The Hospital District will publish a press release in all local newspapers regarding the project and invite any contractors to submit a bid on the project. Additionally, the Hospital District holds the right to reach out to contractors and invite them to bid on any project.

The press release will include, at minimum, the following information:

- The scope and estimated total cost of the public works project
- An explanation of public works projects and a disclaimer regarding prevailing wage, along with a link to L&I's prevailing wage information
- Individual to contact for further information on the project
- The contact information for where to submit bids and the name of the Public Works Project Coordinator

For a contractor's bid to be accepted on any public works project for the Hospital District, they must meet the standards set forth in RCW 39.04.350 that define a "responsible bidder", listed below:

*(a) At the time of bid submittal, have a certificate of registration in compliance with chapter 18.27 RCW;*

*(b) Have a current state unified business identifier number;*

*(c) If applicable, have industrial insurance coverage for the bidder's employees working in Washington as required in Title 51 RCW; an employment security department number as required in Title 50 RCW; and a state excise tax registration number as required in Title 82 RCW;*

*(d) Not be disqualified from bidding on any public works contract under RCW 39.06.010 or 39.12.065(3);*

*(e) If bidding on a public works project subject to the apprenticeship utilization requirements in RCW 39.04.320, not have been found out of compliance by the Washington state apprenticeship and training council for working apprentices out of ratio, without appropriate supervision, or outside their approved work processes as*

*outlined in their standards of apprenticeship under chapter 49.04 RCW for the one-year period immediately preceding the date of the bid solicitation;*

*(f) Have received training on the requirements related to public works and prevailing wage under this chapter and chapter 39.12 RCW. The bidder must designate a person or persons to be trained on these requirements. The training must be provided by the department of labor and industries or by a training provider whose curriculum is approved by the department. The department, in consultation with the prevailing wage advisory committee, must determine the length of the training. Bidders that have completed three or more public works projects and have had a valid business license in Washington for three or more years are exempt from this subsection. The department of labor and industries must keep records of entities that have satisfied the training requirement or are exempt and make the records available on its website. Responsible parties may rely on the records made available by the department regarding satisfaction of the training requirement or exemption; and*

*(g) Within the three-year period immediately preceding the date of the bid solicitation, not have been determined by a final and binding citation and notice of assessment issued by the department of labor and industries or through a civil judgment entered by a court of limited or general jurisdiction to have willfully violated, as defined in RCW 49.48.082, any provision of chapter 49.46, 49.48, or 49.52 RCW*

In addition to the "responsible bidder" criteria set forth in RCW 39.04.350, the Hospital District also requires any bidder to meet the following condition(s):

- Previous experience in the main trade involved in the project. For projects totaling more than $20,000, the bidder must be able to provide a project portfolio of previous work as well as documentation in the form of training, references, or degrees that support their ability to successfully complete all tasks within the project **upon request**.
- A bond is required for projects totaling more than $15,000, unless classified as an Emergency Project.
- All secondary subcontractors must be listed on the bid; all secondary subcontractors must meet the listed criteria and qualify as a "responsible bidder".

The primary contractor who submits the lowest bid and is found in compliance with all the regulations set forth in this policy will be awarded the contract for the public works project at hand.

**Small Works Projects**

For projects totaling less than $350,000, the District's Board of Commissioners has elected to use MRSC's Small Works roster, adopted in resolution # 23-585.

For small works projects, Washington State has mandated that public agencies can forgo the bidding process in exchange for securing quotations from responsible bidders from the Small Works Roster, stated under RCW 39.04.155.

For projects totaling less than $75,000, the District will select the most suitable contractor from the Small Works Roster. For projects totaling less than $350,000, the District must secure a minimum of five quotations.

All quotations should be submitted from contractors currently registered on the MRSC's Public Works roster, upon request from the District. The Public Works Project Coordinator is responsible for reaching out to contractors from the roster via email or phone and securing bids via email. All bids submitted by contractors must be received in PDF format.

**Emergency Work**

The bidding process may be waived, regardless of cost only under the circumstances of an emergency. An "emergency" is defined by Washington State under RCW 39.04.280 as, "emergency" means unforeseen circumstances beyond the control of the municipality that either: (a) Present a real, immediate threat to the proper performance of essential functions; or (b) will likely result in material loss or damage to property, bodily injury, or loss of life if immediate action is not taken."

Emergency work may be awarded to the first contractor who is able to respond to the emergency and meets the minimum requirements listed for a responsible contractor.

**Ordinary Maintenance**

L&I defines ordinary maintenance as, "maintenance work performed by the regular employees of the state or any county municipality, or political subdivision created by its laws". Project considered ordinary maintenance do not need to undergo the bidding process, regardless of cost.

Projects that would be considered ordinary maintenance include the maintenance and repair of existing facilities and goods. Any project that requires specific repair, materials, or supplies does not qualify under the category of "ordinary maintenance". Examples of ordinary maintenance include:

- Cleaning of gutters and windows
- Mowing the lawn
- Services an A/C unit or a generator

**Contracting**

*Contracting Proceeding Formal Bidding*

For all public works projects with contractors selected through the formal bidding process, the Administrator or Superintendent will request a custom contract from legal counsel. The contract will include, at minimum, the following information:

- Name, UBI, Mailing Address, and Contact Information for the lowest bid contractor.
- Total Estimated Cost of Project
- Blueprints/Architectural Outline for the project (if applicable)
- Wage Rates and a link to the prevailing wage rates lookup page on L&I's website

- Contact Information for the project lead at the contracted agency, the Hospital District, and the Public Works Coordinator
- Bonding requirements for the public works project

*Contracting Proceeding Small Works Bidding*

For public works projects with contractors selected through MRSC's Small Works Roster, the Public Works Project Coordinator will develop a contract from the General Small Works Contract Form.

All contracts developed for Small Works must include the minimum required information listed under formal bidding.

*Contracting for Emergency Work*

A contract is not required for emergency work.

**Bonding**

For small works projects, bonds may be required at the District's discretion. For projects exceeding $350,000, bonds are required for any project.

Bonds ensure that the agency will be protected from contractor error, incompletion, or funding concerns. Bonds must be secured by the contractor on behalf of the agency. Fees incurred throughout the bonding process will be paid by the Hospital District, upon reimbursement request from the contractor.

**Prevailing Wages**

The Hospital District will pay prevailing wages to any laborer or apprentice who works on a public works project for the District under a profession classified under the "Scopes of Work" tab on the Washington State Labor and Industries website who is not an employee of the District.

The prevailing wage(s) appropriate for the affiliated public works project will be classified and wages identified within the contract between the public agency and the contractor and will follow the subsequent regulations:

- All contractors are responsible for completing and filing the Intent to Pay Prevailing Wages, Affidavit of Prevailing Wages Paid, and submitting Certified Payroll Records through Labor and Industry's website.
- All laborers will be paid by *type* of work, not their job title. Contractors are responsible for ensuring that hours are documented appropriately and submitted to the public agency for review and approval upon completion of the project.

The Hospital District will withhold 5% of any payment to the contractor until the Intent to Pay Prevailing Wages, Affidavit of Prevailing Wages Paid, and Certified Payroll Records have been documented and approved on the Washington State Labor & Industries website.

### A.12.8 Prevailing Wages

According to the Washington State Prevailing Wages on Public Works Act, public agencies undergoing any public works project must pay prevailing wages to laborers that are not directly employed by the public agency. As a publicly funded agency, the hospital district must comply with Washington State Prevailing Wage Laws. Prevailing wages will be determined by the due date of the bid or the signed contract, dependent upon the project and based on Washington State's rates for the date.

Procedures for "Prevailing Wages"

Prevailing wages will be paid to any contractor working on a public works project for the hospital District. A public works project is defined by Washington State as any work that encompasses:

- Building service maintenance (janitorial) contracts
- Landscape construction and grounds maintenance
- Small projects (no minimum dollar amount) such as maintenance and repairs including "small works" roster contracts
- Off-site work such as custom fabrication for the public works project

All contractors working on public works projects with a total budget greater than $15,000 will be responsible for submitting a bid for work to the Hospital District.

Contractors working for the District are responsible for complying with all prevailing wage laws throughout the bidding, contracting, operation, and conclusion of the project. This includes filing the Statement of Intent to Pay Prevailing Wages, filing Certified Payroll Reports no less than once a month, and completing and submitted the Affidavit of Wages Paid upon completion of the project to Washington State L&I.

The District will not provide payment for services until the Statement of Intent to Pay Prevailing Wages has been submitted and approved by L&I. Additionally, the District will withhold 5% of total payment for a public works projects greater than $15,000 in total upon completion of the project until the Affidavit of Wages Paid has been submitted and approved by L&I.

## A.13 CORPORATE HONESTY AND INTEGRITY

### A.13.1 Conflict of Interest

The District's reputation for honesty and integrity is critical to its continued success. This section governs conflict of interests regarding the District, the District Board, and District employees. This section is intended to comply with HRSA Federal Financial Assistance Conflict of Interest Policy; 45 CFR §75.112; and 45 CFR §75.327(c)(1).

A "Conflict of Interest" is considered a significant financial interest that could directly compromise or bias professional judgment and objectivity related to the management of federal financial assistance.

### A.13.2 Honesty and Integrity of the Board of Commissioners

The District has previously adopted:

(1) Bylaws (most recently amended June 28, 2018) (the Bylaws); and
(2) Board of Commissioners Code of Ethics (established July 30, 2014, and approved by the District Board on November 19, 2014) (the Code of Ethics).

Both the above documents include policies and procedures which govern conflicts of interest for Commissioners and the District Board. This section hereby adopts and incorporates by reference the Bylaws and Code of Ethics as amended from time to time.

### A.13.3 Honesty and Integrity of Employees

Each employee will protect the District's reputation through ethical and honest relationships with the public, suppliers, consultants, the Commissioners, other county, state and local entities and employees and each other within the District. Employees are prohibited from misrepresenting facts or making promises on behalf of the District without prior written approval of the Superintendent and/or Resolution of the District Board.

Procedures for Honesty and Integrity of Employees

Examples of conditions under which outside activities, relationships, or financial interests constitute a conflict of interest include but are not limited to:

1. Activities constituting violations of anti-trust and anti-kickback laws;
2. Accepting or offering items of value from suppliers, patients, or consultants designed to influence treatment, future Board decisions or other similar considerations;
3. Charging or paying more or less than fair market value for goods and services from entities which make or accept referrals from the organization;
4. Using one's position for the purposes of being or appearing to be motivated by a desire for financial gain for themselves, their family, their businesses, or other ties; and/or
5. Entering into financial obligations or investments which could have the appearance of taking advantage of insider knowledge or a conflict of interest.

At the time of employees' hire, each employee shall disclose in writing to the District Board all personal and/or professional relationships that create, or have the appearance of creating, a conflict of interest with the District. Should any such personal or professional relationships arise in the future, the employee shall promptly disclose such relationships to the District Board.

If outside activities do arise either by the employee or their family which contradict these rules, the employee must supply in writing to the District Board an explanation of the activity and the course the employee is going to take to ensure that the situation is resolved.

If Federal, State, Local and/or private grants are used, the District shall ensure that all subrecipients, subcontractors, management and consultants likewise take reasonable steps to ensure the subrecipients, subcontractors, management and consultants also

comply with this section in full. As soon as the District has become aware that any conflict of interest has been breached or has the potential to do so, the District shall contact the respective rewarding agency or pass-through entity.

Questions regarding the propriety of any offers made or solicited by vendors, consultants or subcontractors should be referred to the Superintendent, who may seek legal counsel regarding the propriety of the offers. In addition, any violation of federal, state, or local criminal law, including, but not limited to, fraud, bribery, and gratuity, will be reported as soon as practicable to the Superintendent, the District Board, and the funding agencies that may be impacted by the illegal activity.

Any employee found in violation of this section shall be disciplined in accordance with the policies as set forth in section P.11 Discipline.

## A.14 DATA SECURITY

See also section P.10 Information Technology Appropriate Use Policy.

To maintain high security of data and assets, the District retained the services of NW Tech as its IT help desk and maintenance providers. NW Tech monitors the District's firewall, provides technical assistance, including the managing of programs, the structure of, security of, and access to the District's file system and care for the various devices of the District. This provision of services is also provided to all devices purchased using Federal, State, and County funds and all software and data stored on those devices for the purposes for which they were intended.

Procedures for "Secure Management of Data"

Employees shall not:

- Share their login ID or password information with anyone else unless authorized to do so by the Agency Head;
- Use the District's electronic assets or file systems for any purpose other than the work provided by the District for its own needs or to administer the various grants and entities with which the District is involved;
- Use any personal devices which rely on file systems outside of the District's control to save, manipulate, share or otherwise work on sensitive and confidential data unless authorized to do so by the Superintendent in the normal course of business; nor
- Compromise the security or confidentiality of the files and data of the District by allowing unsupervised use the District's computer or electronic equipment to anyone not employed by the District

However, these provisions should not in any way be construed so as to prevent an employee from saving information for the purpose of preventing or uncovering fraud and/or abuse of Federal, State or County funds and/or property.

The account with NW Technologies is audited every five years to ensure compliance with SAM, and to ensure that costs for services remain competitive.

## A.15 EXPENDITURE REIMBURSEMENT: MEALS, AWARDS, TRAVEL, AND MILEAGE RULES

### A.15.1 Policy

It is the policy of the District that employees should be reimbursed for reasonable expenses incurred in the conduct of District business, including travel for District business and certain non-travel meals and events at which District business is conducted. "Reasonable" is interpreted considering Federal and State statute and guidelines, actual and practical costs, and the recognition that District travel is paid with public funds. Additionally, budgetary constraints and available cash will be considered.

The Board approves overall budget amounts for travel expenses, meals, etc., but ultimately, many decisions as to the reasonableness of travel and meal expenditures are left to the discretion of the Agency Head or Superintendent. Reimbursement only applies to an employee or volunteer doing work for the District.

Contractors and non-personnel may be reimbursed for travel and meal expenses consistent with a service contract and as negotiated with the Agency Head or Superintendent, and do not need to mirror this policy. In such cases the District will generally opt for a single "all in" rate that includes an estimate of total daily costs and is paid in one lump sum.

Where possible, the District opts to assign a set per diem rate consistent with RCW 42.24.090.

### A.15.2 Travel Authorization

Advance approval by the Agency Head or the Superintendent is required for travel, with a cost estimate made before travelling.

Procedures for "Travel Authorization"

Approval will be based on the following criteria:

- Travel is within the mission of the District
- Travel is within the scope of the position of personnel traveling
- Travel is within budget, including temporary restrictions on expenditures

The expenses will be reimbursed using the following guidelines:

- All travel and meal expenses must be preapproved by the Agency Head or Superintendent
- Approval will be based on individual and organizational needs assessment and budgetary status

### A.15.3 Travel Reimbursement

Employees are responsible for commuting expenses to and from their normal place of employment. If an employee has multiple "regular workplaces"—and travel is required between locations on any given day—transportation expenses are reimbursable expenses.

Travel expenses that have been approved by the Agency Head or Superintendent should be reimbursed provided that the employee has the proper documentation and has followed the policies and procedures, as applicable, for travel reimbursement.

Procedures for “Travel Reimbursement”

**Reimbursement Procedure**

Employees may be reimbursed after traveling or given an advance (an advance shall only be allowed for per diem fees, which are fixed based on days of travel). Either way, a full trip itinerary and reimbursement form shall be submitted outlining the cost to the District before travelling.

All travel expenses must be cleared with the Agency Head or Superintendent before travelling. After traveling, an expense report is filled out by the employee and signed. Receipts will be submitted for any non per diem expenses. Any expenses already advanced the employee will be deducted out of the reimbursement.

**Travel by Private Vehicle (set per diem rate)**

Travel by personal vehicle is reimbursed by mileage:

- Properly insured privately-owned vehicles may be used for official travel
- The District will reimburse employees for the use of private vehicles on District business when pre-approved
- The 2025 rate is $0.70 per mile. This rate is pegged to the most recent General Services Administration rates and can be found at gsa.gov/mileage, but where the GSA and this policy differ, this policy will be followed until updated.
- Documentation of mileage should be provided for reimbursement
- Gas is not separately reimbursed, this per diem rate is intended to consider cars that vary in gas mileage, insurance costs, vehicle maintenance, equivalent car rental fees, etc.
- Two or more employees traveling to the same location on District business will travel in one car where possible, with multiple vehicles used when the first is full, however, where travel is taking place as a group an employee may opt to travel on their own with permission from the Agency Head or Superintendent, but are not eligible for mileage reimbursement.

**Travel by Airline (actual cost reimbursement)**

Travel is reimbursed for the flight at the ticket cost.

Tickets should be for coach class and priced reasonably in the Agency Head or Superintendent. Travel by small plane may also occasionally be necessary, and sometimes more cost-effective than travel by vehicle and ferry.

**Lodging (generally a set per diem rate)**

- $175 per diem generally
- $220 per diem for a major metropolitan area such as Seattle, Everett, or the Vancouver/Portland area or a high tourism area where lodging is expensive such as Orcas Island. Requires approval by Agency Head or Superintendent.

- For out-of-state travel, conferences, or District-arranged travel, the District may opt for actual reimbursement rather than a per diem (or the District may pay directly). In such cases a receipt should be provided.

Employees receive a per diem for hotel and incidentals, except when travelling to a major metropolitan area such as Seattle, Everett, or the Vancouver/Portland area or a high tourism area where lodging is expensive such as Orcas Island (as approved by the Agency Head or Superintendent). This per diem rate is simplified and adapted from the Washington State per diem rates and staff research on costs; they should be adjusted each year to keep pace with costs.

Where these rules are not a good fit such as for a conference with a set fee, or where a group of employees are traveling together and the District arranges the travel, the Agency Head or Superintendent may opt to have the District pay directly or reimburse the employee at cost, at the employer's option. In such cases the employee will not receive the lodging per diem. Generally, each employee should have their own room, but up to two same-sex employees may be required to share a room in certain circumstances.

An employee should be able to stay reasonably close to the place they will be working (less than 20 minutes away). Employees are not expected to stay outside of the Seattle, for instance, to save money. Employee time and travel also costs money and should be considered when making lodging decisions.

**Travel Meals (generally a set per diem rate)**

Travel meals are reimbursed as a set per diem allowance rather than actual cost. Non-Travel Meals and Food are covered elsewhere.

Current 2026 rates for meals (adapted from the General Services Administration rates) are: $22 for breakfast, $26 for lunch, and $38 for dinner. The employee will be paid a "per diem" when travelling based on the number of meals required. Partial days will be reimbursed as outlined below.

Receipts do not need to be provided to receive the per diem. Also, the employee should obviously not use a district credit card for meals when receiving a per diem.

If meals are expected to cost more than the per diem allows, approval is required from the Agency Head or superintendent and receipts must be tracked. If personnel attend a business meal at which a fixed per-person price is charged, the employee will be reimbursed the full cost of that meal, when documentation is provided.

On the first and last day of travel:

- If travel time begins before 9:30 am, the employee is eligible for reimbursement for breakfast.
- If travel time occurs between 11:30 am and 1:30 pm, the employee is eligible for reimbursement for lunch.
- If travel time extends after 5 pm, the employee is eligible for reimbursement for dinner.

On all other travel days, the employee is eligible for reimbursement for breakfast, lunch, and dinner except when a hotel provides a full breakfast, in which case the breakfast per diem should not be paid to the employee (a continental breakfast does not count).

**Ferry Travel (actual cost reimbursement)**

Travel on Washington State Ferries (WSF) requires a receipt. It is acceptable to use a personal multi-use pass to save the district money, but verification from WSF that the pass was used should be provided. Reimbursement will be equal to the actual cost to the employee per ride on the multi-use pass. Use of the District account with WSF is also acceptable where applicable.

**Miscellaneous Expenses (actual cost reimbursement)**

Other incidental expenses should be tracked, and receipts kept, and a reason for incurring the expense documented.

The following miscellaneous expenses are reimbursable without receipts:

- Day parking fees
- Mass transit fares
- Bridge Tolls

The following expenses are not reimbursable:

- Valet services such as bellhops, laundry, etc., except where required (e.g. a restaurant that requires valet services)
- Alcoholic beverages, with no exceptions
- Personal phone calls, unless to advise family members of a change in travel plans
- Entertainment expenses, such as movie rentals or show entries

### A.15.4 Compensability of Travel Time

Travel time is compensated consistent with guidelines established by the Fair Labor Standards Board (FLSB).

Procedures for "Compensability of Travel Time"

**One-Day Trips**

One-day trips are managed as follows:

- Hourly pay starts at the time the employee leaves the home or the workplace, whichever is closer to the ferry terminal, airport, or other point of departure
- Hourly pay stops at the time the employee returns home or to the workplace, whichever is closer to the ferry terminal, airport, or other point of departure

**Overnight Trips**

Hourly pay is calculated by the following guidelines:

- Starts at the time the employee leaves the home or the workplace, whichever is closer to the ferry terminal, airport, or other point of departure
- Hourly pay stops at the end of the official meetings for day 1, or when employee arrives at the destination for the meetings
- Hourly pay starts again when the meeting starts on day 2, or, if no meeting, when the person begins travel back to the home island
- Hourly pay stops on day 2 (and subsequent days) at the conclusion of the day's meetings, if the employee is not returning home that day; or, if the employee is returning home that day, at the time the employee returns to the home or workplace, whichever is closer to the ferry terminal, airport, or other point of departure
- Time spent at conference meals is not compensable

Notwithstanding the above, the employee shall be deemed to have worked at least 8 hours on any day during which he or she is away from home the entire day.

### A.15.5 Employee Expenses and Expense Reimbursements

It is the Agency Head or Superintendent's responsibility to sponsor events that serve the public interest and to keep it within the overall budget set by the Board of Commissioners. All such non-travel meals and food must be approved by the Superintendent or Agency Head, and be consistent with the approved budget by the Board of Commissioners.

Working meals can be efficient for the District generating extra hours worked by employees whose hourly wage often exceeds the cost of the meal, who otherwise would not have worked the meal hour, and may in any case be on salary or on call. It can also be a wonderful way to advance the purposes of the District with key partners and develop key relationships. However, excess should be avoided and care taken to document reasons for the meal.

Procedures for "Non-Travel Meals And Food"

Non-travel meals are reimbursed based on cost, and receipts must be provided:

- Meals will be reimbursed at actual cost based on receipts
- Excessively expensive meals should be avoided, though the District recognizes that there are increasingly few options on San Juan Island
- Gratuity of around 20% are reimbursable subject to the per diem limits. Over the COVID years, socially acceptable minimum tip rates have gone up, and paying less than 15% should be avoided.
- The District may pay for meals for people who are not employees or volunteers, but only if the purpose of the meal is to promote the interests of the hospital district in a meaningful and concrete way. This should be documented on the receipt or request for reimbursement.
- Follow the "no four-star hotels" rule of thumb: if it's a premium, top tier restaurant it should be avoided

**Meals at Employee Meetings**

The District may provide food and/or meals at staff meetings, work meetings, or other employee events such as training under the following circumstances:

- The purpose of the meeting is to conduct official District business or to provide training to District employees or officials; and
- The meal is an integral part of the business meeting or training session (that is, business and/or training are conducted during the meal); and Reimbursement for approved meals will be at actual cost, not to exceed current per diem rates.

**Meals at Meetings of Boards, Commissions, Job Interviews, etc.**

Meals may be provided for meetings of advisory boards, all agency training sessions, job interviews, board of commissioners, staff meetings, etc., under the following circumstances:

- The purpose of the meeting is to conduct official District business
- The meeting extends through normal mealtimes for the convenience of the District
- Business is conducted during the meal
- Reimbursement for meals will be at actual cost or paid directly by the District

The Superintendent or Agency Head will determine the appropriate extent of the expenditure.

**Employee/Volunteer Recognition Events and Awards**

*Elections* – No expenses will be reimbursed for events held to celebrate elections, and agency resources such as the building should not be used for that purpose.

*New Staff* – The District may hold an event to allow personnel and their families to meet new management staff as this may improve engagement and cooperation within the District during what can often be a stressful time for staff. Refreshments may be provided, not to exceed normal limits for meals per person

*Retirements* – The District does not normally hold retirement parties, though the Superintendent may make an exception where the employee in question played a public role significant enough to justify including the public, in which cases light refreshments may be provided and a venue for the public to attend. Separately, the District's offices may be used for a retirement party at the option of the Agency Head or Superintendent, but food will not be paid for by the District (e.g. the EMT Association pays for food and decorations but the District provides the venue).

*Service Anniversaries* – Employees who have achieved five-year service anniversary intervals with the District during the current year may be recognized at a Council meeting or staff meeting, and refreshments may be served not to exceed normal limits.

*Annual Events* – An employee appreciation event, to which all employees of a specific agency, department, or division are invited(and may or may not include one guest per person), and which may include a meal, may be held once annually per agency or as a District. The District may contribute up to $100 per employee or volunteer for this event (but still must be approved and managed through the normal budget and expenditure process). A nominal gift of appreciation may be purchased for years of employment or for recognition of service.

In general, most employees have an assigned team, such as Village at the Harbor, or San Juan Island EMS. Certain employees may be invited to more than one event if they have a direct reason approved by the Superintendent. For instance, senior leadership should attend both their agency's function so that they can recognize their employees and then attend with administration so that they themselves can be recognized.

*Awards* – small awards or plaques may be awarded for special services, e.g. the annual Chief's Award, or Employee of the Year. This can promote morale, promote good performance, and is a low-cost way to advance the interests of the hospital district, especially with volunteers.

**Public Celebrations**

Light refreshments may be served at public celebrations, such as the dedication of a building, recognition of major award, or at public meetings with a public purpose. All such events must be approved in advance by the Agency Head or Superintendent.

**Grant-Funded Events**

In some cases, grants specifically encourage the provision of food at public outreach events. Where grant funds are to be so used, the expenditure must fall within current per diem rates, and must be either approved in writing by the granting agency prior to a specific event or generally authorized in the grant contract or administrative rules. A copy of the letter of approval or authorization must accompany request for payment or reimbursement of expenses.

**Scheduled OTEP Training Reimbursement**

Generally, scheduled OTEP trainings are during dinner time. Due to this, the District allows employees and volunteers to provide meals for the group at the District expense. Reimbursement is set at a flat rate of $120 per training. The employee or volunteer who purchases food for the OTEP training is responsible for completing an OTEP Reimbursement form and submitting it to the Finance Department for review.

Unscheduled shift training is not preauthorized for meal reimbursement. Specifically, only OTEP has a stipend reimbursement.

The Training Officer may opt to provide or approve food for trainings as approved by the Chief/Agency Head.

The Chief/Agency Head may permanently change this stipend by updating this procedure.

The Chief/Agency Head may approve a different, temporary stipend by notating approval on a reimbursement request.

**Hosting Events**

Unless one of the types of events elsewhere in this section applies, the District generally does not host events with food for non-personnel. However, there may be times when it is

in the interest of good government and good partner relations to host non-personnel at special events.

Hosting events may not be for the purpose of lobbying a legislator or other governmental official and may not be primarily social events.

Hosting events must be approved in advance by the Agency Head or Superintendent, and the request for payment or reimbursement must include who was hosted, the number of persons in attendance, the location of the meeting, and the business purpose of the meeting.

Examples might include job interviews, multi-disciplinary work groups, working retreats, partnership meetings with PeaceHealth, etc.

**Reimbursement of Expenses**

All reimbursable expenses including transportation must be submitted on the agency expense reimbursement form. Original receipts are required for all expenses except as previously noted. For meals, documentation must show individual items, list of those included in meal, purpose of meal and the total. Credit card receipts or credit card statements that show only the total amount are not adequate and may be rejected for refund.

State regulatory requirements require specific wording, which should be included on the claim of expense: "I hereby certify under penalty of perjury that this is a true and correct claim for necessary expenses incurred by me and that no payment has been received by me on account thereof."

### A.15.6 Moving Expenses

Consistent with RCW 42.24.170, the Agency Head or Superintendent may authorize moving expenses for new hires consistent with the budget and/or a separate Board approval.

Note that this, as of 2022, is a taxable benefit and should be paid through payroll.

### A.15.7 Tuition

The District may budget for and provide tuition reimbursement to employees on a case-by-case basis where it serves the interest of the District. To qualify for tuition reimbursement, the employee's education must meet the following criteria:

- The education must be through an accredited certification program, college, or university.
- The education must offer growth in the employees' current position or offer the training and/or education necessary for promotional opportunities within the company.
- The employee must secure a passing score of 80% or higher in all courses paid for by San Juan County Public Hospital District No. 1.

The employee must sign a contract that makes a commitment to stay for a period of time or be obligated to pay the money back. This may be tiered, for example: the employee must repay 80% if the employee leaves within one year of completion or does not complete the course, 50% if the

employee leaves within two years of completion, and 30% if the employee leaves within one year of completion. Forgiveness terms may be included should the student not complete the program due to unusual hardship or termination.

The employee must:

- Be a full-time employee working at least 32 hours per week
- Provide a copy of transcripts or certification upon completion of the class, proving that the employee maintained the required passing score(s).
- Obtain written approval and sign a contract to be eligible

The Superintendent is the only person who may offer tuition reimbursement to employees and will offer terms and a contract consistent with budget authority. The contract should include terms and conditions such as how the money will be disbursed (stipend, reimbursement, wages, etc.), whether study time is compensable hours (and if so, how much), repayment terms in the event of early separation, etc. There is no set way contractual terms must be set and they are worked out on a case by case basis by the Superintendent with legal counsel.

**A.15.8 Training Agreements and Contracts**

The District provides employees with training to ensure that they can successfully perform their job functions.

All Residential Assistants and Medication Technicians employed at Village at the Harbor are required to be a licensed Home Care Aid (HCA). Likewise, EMTs and Paramedics must obtain and receive training in order to be credentialed for the work they perform.

Unless previously obtained by the employee, this training is provided at the expense of the District. As such, the District requires that employees receiving training may be required to satisfy a number of employment hours for the District in exchange for their training.

Procedure for "Training Contracts"

Employees who receive training through the District may be required to pay or repay expenditures related to their training should they quit before the District can regain the value expended in providing the training. If the employee is expected to pay out of pocket for training, this training may be reimbursed when certain conditions are met.

See also section A.15.7 Tuition

**Assisted Living and Home Care Training**

For Home Care Aides (HCA), this contract will have, at minimum, the following conditions:

- Employees are required to complete six months of full-time employment, or the part-time equivalent, with the District in exchange for their HCA certification.
- Employees must complete the required training for their HCA certification within the first month of their employment with the District.
- If an employee does not satisfy the District's employment requirements in exchange for their HCA certification, including the conditions outlined above, the employee may be

required to refund the cost of the training to the District, per the contract they sign at the beginning of their employment with the District.
- Failure to complete the HCA certification required for their position may result in termination.
- Where Employee is required to refund training costs to the District, Employees agree and consent to the District's garnishment of Employees' wages, including but not limited to Employees' last paycheck, in order to recoup any training costs unpaid by Employees.

**EMT and Paramedic Training**

EMTs trained by the District may be expected to purchase their own books and equipment. The District may offer to reimburse these expenses upon completion of the training.

Paramedic trainees sponsored by the District to go to paramedic school will be expected to sign a contract negotiated with the District to repay costs should the employee quit before a certain period of time has passed, usually 3-5 years.

**Other Employees**

Certain employees may be offered educational opportunities to support their performance as employees, such as master's degrees or other job training. These opportunities will include a contract to repay expenses similar to the paramedic candidate should the employee quit before a certain period of time has passed.

## A.16 FEDERAL GRANT REPORTING OBLIGATIONS

In addition to any of the policies herein, the Superintendent or their grant management designee shall ensure on a regular basis that the District is in full compliance with all the restrictions, limitations, and exceptions as mandated by the Consolidated Appropriations Act, 2021 (Public Law 116-260), as laid out in the HRSA Grants Policy Bulletin number 2021-03 (Grants Policy Bulletin) , the Notices of Award, and any and all future updates or replacements.

However, as stated in the Grants Policy Bulletin, the District shall not require employees to enter into any confidentiality agreements which would seek to prevent employees or contractors from reporting fraud, waste or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information. Furthermore, the District shall not enter into any contract, grant or cooperative agreement with an entity, subrecipient or subcontractor that requires their employees to do so.

The District shall review its policies and procedures annually to ensure continued compliance with any Federal regulations and mandates.

## A.17 HOLIDAY DECORATIONS AND PURCHASES

As a small-town District, the District's main facilities are prominent public buildings that add to the character of the Town. As the Town of Friday Harbor participates in lighting and decorating its buildings, this guideline serves to give guidance as to our appropriate participation in various holidays and to state acceptable expenditures.

1. It is appropriate for a modicum of provision for the holiday lighting and community celebrations that take place around national holidays.
2. At no time shall religious artifacts or ornamentation be purchased by the agency. Individual employees may choose to display religious artifacts in their own personal desk space as long as they do not detract from the work of the agency or cause distraction for others.
3. The District shall set an annual limits in the budget for the purchase and display of non-religious holiday building lighting and ornamentation, such as July 4th and Winter Holidays.

In Village at the Harbor, it is reasonable and appropriate to decorate for holidays that are celebrated by Village residents. Any resident who feels their own traditions are inadequately represented should contact the Administrator. Religious decorations should not be purchased by the District, but displays may be allowed for residents' religious decorations on a temporary basis.

## A.18 HOURS OF OPERATION

Each facility maintains its own hours of operation, set by the Agency Head. Each facility also sets its own hours for members of the public, guests, and holidays. The Superintendent retains overall authority to decide these issues, but they are generally delegated to Agency Heads.

Procedures for "Hours of Operation"

Hours of operation will be posted on the appropriate agency website.

## A.19 INFECTIOUS DISEASE CONTROL

The District complies with all Federal, State, and local regulatory requirements regarding infectious disease prevention. Each agency maintains its own industry-specific procedures for infectious disease prevention. It is the Agency Head's responsibility to make decisions regarding these issues, reporting through the normal chain of command to the Superintendent.

The hospital district complies with state vaccine mandates.

Procedures for "Infectious Disease Control"

Each agency should utilize standing orders regarding COVID-19 precautions as the environment can change frequently and quickly.

Each agency should also maintain its own procedures and standing orders on all other infectious disease issues not outlined in this policy or procedure.

**Handwashing.**

Handwashing is the most important method of infection control.Hands must be washed between direct contact with any residents (Village) or patients (EMS), after doing cleaning tasks, after using the restroom or any other task that provides opportunity for infection.

- Gloves must be worn when coming in contact with blood or body secretions.
- Employees should not work when they are infectious.
- Residents should remain in their apartments when they have a communicable disease.

Hands should be washed using the following process:

1. Turn on water and wash hands with soap. NOTE: It is not necessary to use hot water. Hot water will dry out your hands more quickly. What is most important is good friction and soap. Wash your palm, fingers, between fingers, under fingernails, wrists and forearms.
2. For routine washing, wash the hands for 15-30 seconds. If you feel you are contaminated, wash hands longer.
3. Hold hands downward while washing to prevent germs from contaminating the arms.
4. Rinse hands and wrists well removing all soap and dirt.
5. Dry hands with a clean paper towel.
6. Using the paper towel, turn off the faucet. (Don't use your hands to turn off the water as they are clean and the faucet is contaminated.)
7. Use hand lotion if needed to keep your skin from drying out.

**Standard Precautions**

1. Hands must be washed between any task which has the possibility of transferring bacteria
2. When having direct contact or the potential for direct contact with any body fluids, gloves must be worn.
3. Gloves must be discarded when moving from resident to resident.
4. Wash hands and change gloves when moving from one task to another in the resident's dwelling unit.
5. Use gloves when cleaning areas that may have had contact with body fluids.
6. Use gloves when handling soiled clothing.
7. Eye protection should be worn if there is any risk of airborne illness or any possibility of bodily fluid exposure to the face

## A.20 PAYROLL – GENERAL POLICIES

### A.20.1 General

Please reference the Personnel Policies and Procedures for compensation matters. The goal of this policy is to establish fair and accountable payroll policies.

As a general matter, Human Resources prepares Payroll using timesheets approved by supervisors. The payroll packets are approved by the Finance Director or the Superintendent.

### A.20.2 Timesheet Approval Process

Human Resources will post an annual payroll calendar prior to start of the year. Timesheets are submitted and tracked through TylerTech.

Procedures "Timesheet Approval Process"

- Human Resources sends out notification of pay period ending and any deadlines to supervisors.
- Supervisors then communicate the deadlines to employees to ensure review and submission to Human Resources on time.
- Agency Heads will submit all employee status changes such as pay or benefits by the employee status deadline in writing, with the right form, before timesheets are due.
- Employees will fill out their timesheet and submit it on time through TylerTech.
- Employees who do not input their time and submit it by the deadline will be paid based on what their scheduled hours were. Inputting this time becomes the responsibility of the supervisor. For instance, if their hours are in CareSmartz, WhenIWork or Aladtec, the supervisor will enter their hours into Tyler. Repeated failures to do so by an employee may result in discipline.
- Supervisors are checking that hours worked are correctly entered, that employees received their correct overtime premiums, compliance with applicable CBA and FLSA compliance, that every employee has submitted a timesheet, and checks PTO and/or sick leave (part-time employees).
- Once Supervisors have approved time for their direct reports, timesheets will escalate to department heads. Department heads will review and approve. Timesheets then go to Human Resources. If either the Supervisor or the Department Head is gone, Human Resources will manually approve time after a more careful review than is customary.
- Once timesheets have been fully reviewed and approved in TylerTech, Departments will notify Human Resources that their department's timesheets are complete.
- All supervisors must be able to return a phone call within two hours during the day payroll is processed except by prior notice. At least one person from each department must review and approve timesheets regardless of any PTO time or absences.
- In the event that an employee does not report sufficient hours to meet their scheduled hours, PTO will be applied until the obligation is met or PTO is exhausted. If all PTO is exhausted, and the employee has not met the requirements to maintain fulltime status, benefits will not be renewed for the following month and will revert to part-time status. Employee may regain benefits and full-time status with the department head's permission.

**A.20.3 Processing of Payroll by Human Resources**

Payroll is processed by fund, that is, either fund 6511 (EMS) or fund 6521 (General public hospital district). Payroll processing dates for each budget are based on the payroll calendar. Payroll processing takes place by following the payroll processing packet module in Tyler.

Procedures for "Processing of Payroll by Human Resources"

The following steps will be followed in processing of payroll.

- Once notification is received by Human Resources from the Agency Head that timesheets are done, Human Resources, will open the payroll process in TylerTech.
- Load in deductions, base pays (such as gym memberships, long-term disability, etc.). Deductions, base pays, benefits, and employee status/configuration are entered in prior to payroll by the Human Resources.

- Human Resources will check timesheets based on the following considerations: employees have worked minimum hours based on job classification, will check if there are hours entered for each employee, and pay attention should there be anything blatantly wrong. By request, HR may make additional checks but this shouldn't be assumed by department heads. HR will call and ask questions as needed. Human Resources will make sure that all FTE status information is available and correct.
- Human Resources will then select "lock and approve" for timesheets. This ensures that employees do not modify their time after submission. However, all budgets are locked at the same time, so one budget may remain open while being worked on.
- All of the hours worked, benefits, taxes, corrections, and deductions are loaded in by TylerTech as part of the packet process.
- Manual review will now be performed by Human Resources. Any FMLA or PFML leave time, as well as Admin leave, ADA leave, any other manual changes will be made as necessary. Any manual changes/edits must be submitted by agency head in writing. For instance, an email communication about comp time.
- Sick leave for part-time employees is accrued as part of the payroll process packet. PTO is processed separately through its own TylerTech packet during this period by Human Resources. Human Resources will correct any errors as needed.
- Human Resources will review and begin payroll processing.
- Review all employee status changes, such as pay changes, base pays, deductions, etc. HR will review all employee classification rate changes, such as PERS deduction rates, L&I rate changes, etc.
- Will then authorize payroll in TylerTech by selecting "Approve."
- Lock the pay period. At this point, nothing can be changed. Once that is done, checks are cut.
- Checks are printed on MICR-printer using appropriate payroll checks paper. These are not the same as AP check paper.
- Downloads bank draft EFT file from TylerTech, and then upload to Heritage Bank site using template. All templates are managed and approved by Finance Director.
- Direct Deposit notices are sent out via email. Employees who do not provide an email address may download via Employee Self-Serve website (ESS).
- Update Tyler using the last packet process step.
- Human Resources will process the accounts payable portion of payroll consistent with Accounts Payable policies and procedures. This does not need additional approval.
- Department of Retirement Services (DRS) Reporting must be submitted and payment remitted for both budgets within one week of completing the payroll process.

**A.20.4 Employee Account Changes**

All bank account information must be submitted using paper forms and made to Human Resources. Email submissions will not be accepted as they represent risk of identity theft and fraud.

Procedures for "Employee Account Changes"

- When an employee is enrolled with the District, direct deposit information will be added to the employee account in TylerTech by the Human Resources Manager.

- Human Resources will run a prenote on the bank account information to verify the account information is correct.
- Any changes to bank account information must be submitted to Human Resources and a new prenote must be run. Human Resources will make the changes. It can take up to two weeks for this process to be completed.
- Subsequent to a bank account change, the employee will likely need to accept a paper check on a temporary basis.

**A.20.5 Employee Status Changes**

The creation of all job positions within the District requires Superintendent approval and a job description approved by the Superintendent. Filling existing positions, such a replacing staff lost through attrition, is the responsibility of the agency head.

Procedures for "Employee Status Changes"

- Creating an approved position in TylerTech is the responsibility of Human Resources.
- When a position is created, Human Resources will ask the Superintendent what BARS code to use and then configure the position in accordance with TylerTech's requirements.
- When an employee is hired for an approved position, the Agency Head will submit to Human Resources the employee's pay and FTE status in writing. Human Resources will determine if the employee is eligible for benefits and configure the employee on the correct position.
- Any changes to an employee's FTE status, job title or description, or pay, must be submitted by the department head to Human Resources prior to the timesheet deadline to be included in processing for the pay period. All of these items must fall within the constraints set by the approved job description, Collective Bargaining Agreement, or pay scale found in these policies. If they do not, it requires Superintendent approval.
- It is the responsibility of the Agency Head to ensure that they make changes within the constraints of the job descriptions that have been approved. Human Resources will additionally verify employee changes fall within approved job descriptions or have Superintendent approval.

**A.20.6 Payroll Reporting**

Quarterly reports include PFML, WA State long-term care tax, L&I, Unemployment reporting, and Federal Tax Withholding. Most of these are paid through payroll and one is not. Everything except Unemployment reporting is processed through payroll and "expensed" in Tyler at the time of processing. However, these must be printed and mailed on a quarterly basis. Unemployment requires a separate payable packet created by the Human Resources and approved by the Human Resources Manager.

The District has two budgets. Subsequently, quarterly reporting must be done twice each quarter. Once for 6511 (San Juan Island EMS) and 6521 (The Hospital District, which includes Village at the Harbor and Village at Home).

Quarterly reports are completed by the Human Resources Manager. Quarterly reports include Quarter One: January-March (due before April 30), Quarter Two: April-June (due before July 31),

Quarter Three: July-September (before Oct 31), and Quarter Four: October-December (before Jan 31).

### A.20.7 Corrections to Pay

Corrections will be required from time to time. This may be a result of incorrect pay rates, incorrect "base pays," benefits reporting, time entry, etc. The District always seeks to act in good faith while ensuring fairness to the public and employees.

Procedures for "Corrections to Pay"

Corrections may be required either because the District made a mistake, or an employee made a mistake. All corrections are treated in the same way.

- A correction is processed under the direction of Human Resources in TylerTech through the "Payroll Correction Process," and warehoused until the next pay cycle is processed. Corrections are made on the next pay day as part of the next pay cycle.
- In the event of an underpay, that is, the employee received less compensation than they should have, payment will only be remitted outside of standard payroll cycles with explicit approval from the Superintendent. Supervisors will endeavor to catch mistakes at the earliest point of payroll processing to avoid the need for corrections. Supervisors should consider underreporting of time as well as overreporting of time and any other possible mistakes. Supervisors should notify employees of significant changes to their timesheets as a courtesy, where possible.
- Employees are required to repay in full any overpay of compensation by the District. Upon an overpayment, the District will provide the employee with a letter offering them multiple options for repayment, per RCW 49.48.200.
- Per RCW **49.48.200** (1) Debts due the state or a county or city for the overpayment of wages to their respective employees may be recovered by the employer by deductions from subsequent wage payments as provided in RCW **49.48.210**, or by civil action. If the overpayment is recovered by deduction from the employee's subsequent wages, each deduction shall not exceed: (a) Five percent of the employee's disposable earnings in a pay period other than the final pay period; or (b) the amount still outstanding from the employee's disposable earnings in the final pay period. The deductions from wages shall continue until the overpayment is fully recouped. (2) Nothing in this section or RCW **49.48.210** or **49.48.220** prevents: (a) An employee from making payments in excess of the amount specified in subsection (1)(a) of this section to an employer; or (b) an employer and employee from agreeing to a different overpayment amount than that specified in the notice in RCW **49.48.210**(1) or to a method other than a deduction from wages for repayment of the overpayment amount.
- When an employee is required to repay the District, it will comply with all federal minimum wage laws, e.g. employees may not be paid less than federal minimum wage after deductions are applied.

### A.20.8 Payment

Procedures for "Payment"

Employee paychecks and reimbursements will be deposited directly into the employee's account unless other arrangements are made with Human Resources. Funds will be

available for employees consistent with a published payroll calendar each year. Direct deposit provides the greatest assurance that payroll checks will be available to employees on designated pay dates.

Payment will be made to terminated employees at the same time as other employees. The Agency Head should provide the exact time and date that the employee's employment ended, as well as instructions on cash-out of PTO, any administrative leave used, etc.

Any physical checks will be secured in a locked office or drawer until distribution. Checks must be handed directly to the employee or mailed via U.S. Postal Service if requested by the employee.

A check will not be given to any person other than the employee without a phone call from the employee to the Agency Head or Human Resources, granting permission for the Manager to give the check to that person. Additionally, any person picking up a check for an employee must present a photo ID to verify identity or be personally known to the administration employee handing over the check.

## A.21 PUBLIC RECORDS AND RECORD KEEPING

### A.21.1 General

Washington's Public Records Act, Chapter 42.56 Revised Code of Washington (the Act), requires that government agencies adopt rules and procedures relating to maintenance and availability of public records. The District maintains various types of public records relating to its operations and will make available to the public any and all requested public records not exempt under the Act.

Based on the above, the District adopts the following policies and procedures relating to public records and the public's access to the District's public records.

### A.21.2 Access to Public Records

Procedures for "Access to Public Records"

1. **Public Record:** Public records of the District include any writing containing information relating to the conduct or performance of any governmental function prepared, owned, used or retained by the District except records and information exempt from public inspection and copying under the Act.
2. **Public Records Availability:** All public records of the District, as defined above, are available for public inspection and copying pursuant to these procedures, except as otherwise exempt under the Act.
3. **Location of Records:** The records are maintained at the District's building located at:
   535 Market Street, Suite E
   Friday Harbor, WA 98250
4. **Hours for Inspection and Copying:** Public Records shall be available for inspection and copying during the normal office hours of the District which are from 9:30 a.m. to

2:00 p.m. and from 2:30 p.m. to 5:00 p.m., Monday through Thursday, excluding legal holidays, by appointment.

### A.21.3 Public Records Officer

The Public Records Officer will oversee compliance with the Act, although another District employee may process the request. The Public Records Officer, or its designee, and the District will provide the fullest assistance possible to requesters while preventing public records requests from causing excessive interference with the essential functions of the District.

The Public Records Officer is appointed by the Superintendent.

Procedures: "Public Records Officer and Records Requests"

The Public Records Officer can be reached at:

Public Records Officer
San Juan County Public Hospital District No. 1
PO Box 370
Friday Harbor, WA 98250
(360) 378-2857, ext. 201
https://sjcphd.org/contactus/public-records-requests

### A.21.4 Records Requests

In accordance with the provisions of the Act, public records may be inspected and copied, or copies obtained by members of the public by filing a request. Procedures for this as follows:

Procedures for "Records Requests"

1. It is encouraged that public records requests be made in writing to the Public Records Officer and include the following information:
   - The name and address of the person requesting the record.
   - The time of day and calendar date on which the request is made.
   - The nature of the request.
   - If the matter requested is referenced in a current index maintained by the District, a reference to the requested record as it is described in such index.
   - If the requested matter is not identifiable by reference to an index, an appropriate description of the record requested.
2. In all cases in which a member of the public is making a request, it shall be the obligation of the employee to whom the request is made to assist the member of the public in appropriately identifying the public record requested.

For the convenience of the public a request is posted on the District website at https://sjcphd.org/contactus/public-records-requests.

### A.21.5 District's Response to Public Records Requests

Requests for public records will be forwarded to the Public Records Officer, who will review the request and ask the appropriate staff for the records. Upon receipt of the public records request,

either the requested materials or a written response will be provided to the requester within five (5) business days. If the District requires additional time to fulfill the request, the requester will be so notified and provided with a response date.

Procedures for "District's Response to Public Records Requests"

1. **Additional Time is Needed:** The District's response may include a statement that additional time is needed to clarify the intent of the request, more time is required to locate and assemble the requested documents, to notify third persons or agencies affected by the request, or to determine whether any of the documents are exempt and a denial shall be made to all or part of the request. The District shall provide an estimated date by which it expects to will complete its response to the request.
2. **Procedure if Clarification is Needed:** If a request is not specific, or an identifiable record cannot be ascertained from the request, the Public Records Officer may seek clarification from the requester while also giving the request an estimated response time.
3. **Procedure for Notifying Third Parties:** The District occasionally receives records that include potentially exempt sensitive personal or business information from third parties. There are circumstances in which the District, within its discretion, will provide advanced notice to third parties affected by requests for records which may contain sensitive information related to the third party. The information provider (third party) may seek court protection under RCW 42.56.540 by demonstrating that such information would: (a) clearly not be in the public interest; and, (b) substantially and irreparably damage any person; or (c) substantially and irreparably damage vital government functions. The notice to the affected persons will include a copy of the request.
4. **Providing Records in Installments:** When the request is for a large number of records, the Public Records Officer or designee will provide access for inspection and copying in installments, if he or she reasonably determines that it would be practical to provide the records in that way. If within thirty (30) days, the requestor fails to inspect the entire set of records or one or more of the installments, the Public Records Officer or designee may stop searching for the remaining records and close the request. The Public Records Officer will provide the requester with notice that the District will be closing the request.
5. **Request Denial:** If the District determines it is denying the request, in whole or in part, a written statement of the applicable exemptions and specific reasons for the denial shall be provided to the requester. A decision by the District denying inspection will be reviewed by the District attorney prior to the issuance of the denial to the requester. Such review shall constitute final action for the purposes of judicial review. The requester shall be notified of the decision to grant or deny the request. (See below for appeal process.)

6. **Overbroad Requests:** A request for all or substantially all public records of the District is not a valid request for identifiable public records and will be denied. The District may deny a bot request that is one of multiple requests from the requestor to the District within a 24-hour period upon establishing that responding to the requests would cause excessive interference with other essential functions of the District. A "bot request" is a request for public records that the District reasonably believes was automatically generated by a computer program or script.
7. **Later Discovered Documents:** If additional records are discovered that should have been provided as part of an earlier public records request, those documents will be forwarded to the requester as soon as practicable with a brief explanation as to why the newly discovered documents were not located as part of the request response.

### A.21.6 Fees and Charges

Procedures for "Fees and Charges"

1. No fee shall be charged for the inspection of public records. The requester will be notified when the records are ready for inspection and a mutually agreeable time for inspection will be set. The District is not obligated to create or format documents that are not in existence.
2. The District shall charge a fee of 15 cents per page for providing copies of public records. This charge is the amount necessary to reimburse the District for the actual cost of such copying. In the event the District is requested to mail requested copies, an additional charge in the amount of the actual or estimated postage shall me made.

### A.21.7 Exemption from Public Disclosure

The District reserves the right to determine whether a specific requested record is exempt in whole or in part from public inspection under the Act.

1. In accordance with the Act, the District reserves the right to delete identifying details when it makes available any public record in any case where there is reason to believe that disclosure of such details would be an invasion of personal privacy protected by Chapter or the Act.
2. All denials of requests for public records shall be accompanied by an exemption log specifying the reason for the denial, including a description of the record, statement of the specific exemption authorizing the withholding of the record and a brief explanation of how the exemption applies to the record.

### A.21.8 Appeal Process if Request is Denied

The requester may appeal a decision by the District to withhold a document to the District's Public Records Committee. The appeal must be filed within fourteen (14) business days of the date of notification to deny inspection of the requested public record. The Public Records Committee, consisting of the Superintendent, a Commissioner, and a District attorney, will either affirm or

reverse the denial within two (2) business days following the District's receipt of the appeal or within such other time as the District and the requester mutually agree.

## A.22 RECORD RETENTION POLICY

### A.22.1 Purpose

The purpose of this Policy is to establish guidelines for record retention in accordance with 45 CFR §75.302, and all applicable federal, Washington State and local laws. This Policy applies to all San Juan County Public Hospital District #1 employees and officials.

### A.22.2 Definitions

District: is San Juan County Public Hospital District #1.

Public Record means any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. Public Records encompass electronic documents, including Social Media posts, comments, and other records, whether created by computer, tablet, phone, or other electronic device.

Public Records Officer is the District's current, acting Public Records Officer.

Retention Schedule refers to the current Washington State records retention schedule. These retention schedules run in the hundreds of pages and are maintained by Washington State Archives under the Washington Secretary of State.
https://www.sos.wa.gov/archives/recordsmanagement/select-type-of-local-government.aspx

### A.22.3 Policy

All Public Records are required to be retained according to the Retention Schedules set by the State of Washington, regardless of how the record was created:

- If the transaction of public business occurs in paper then the paper record is the primary copy for retention purposes.
- If the transaction of public business occurs electronically then the electronic record is the primary copy for retention purposes.

There are certain records that have little or no retention value versus those records that must be retained as provided herein.

Records with retention value include (but might not be limited to):

- Correspondence or memorandum related to the official business of the District.
- Original reports.
- Policy and procedure directives.
- Agenda and meeting minutes.
- Documents related to legal or audit issues.
- Messages documenting District actions, decisions, operations and responsibilities.
- Documents related to District transactions.

- Appointment calendars.

Records that are not likely Public Records and therefore have no retention value:

- Information-only copies of documents that do not relate directly to the functional responsibility of the District or the agency that receives them.
- Personal messages or announcements not related to the official business of the District (i.e. cake for someone's birthday in the break room).
- Phone message slips that do not contain information related to the official business of the District.

**A.22.4 Electronic Records**

Electronic records must be retained in electronic format for the length of the designated retention period.

- Printing and retaining a hard copy is not a substitute for the electronic version. Metadata associated with "born digital" records establishes the authenticity of the record, providing evidence of the transaction taking place.
- Printing electronic records (e.g. emails) preserves the informational content but not the authenticity of the record and the metadata.

Electronic records and electronic mail should be retained as follows:

- Generally speaking, for records originating within the District, the person who creates and sends the message holds the District record copy.
- For records received from outside the District, the primary recipient or the District recipient taking action holds the District record copy.
- Thereafter, all electronic records and electronic mail should be retained for the length of time prescribed in the Retention Schedule.

**A.22.5 Safeguarding Public Records**

Upon the District's receipt of notice regarding the initiation of an investigation, the service of legal process, or the receipt of a public records request, the Public Records Officer will promptly notify all agencies and individuals in possession of potentially relevant documents and direct them to safeguard all documents pending further notice that the investigation, litigation, or public records request has been concluded. In this regard, no relevant documents should be destroyed until further notice is received.

**A.22.6 Personal Email Accounts**

The use of personal email accounts to conduct District business should be avoided. If you must send an email from a non-District and/or personal account, copy to your District email address at the same time.

If you receive a business-related email on a personal account, forward to your District email address and retain that as a primary copy. You should also retain a copy in your personal account.

### A.22.7 Website

The District retains all web content in accordance with the approved Retention Schedules, this includes design/architecture of website, content of website, and changes to website content.

### A.22.7 Use Of Personal Device

District employees and officials should strive to use District issued devices and accounts to conduct all District business. Records created, received or used on your personal device are Public Records if they are related to the conducting of District business. It may be your personal device or account, but if it's being used for District business you are accessing (and sometimes creating) Public Records. All Public Records on your personal device must be kept in accordance with the Retention Schedule.

### A.22.8 Voicemail

Voicemail messages are Public Records if they relate to the conduct of District business. All voicemails that are Public Records shall be retained according to the Retention Schedule. The following are options for retention:

- Option 1 – Save as an audio file attached to an email.
- Option 2 – Memorialize business transaction in email to sender summarizing content.

### A.22.9 Text Messaging

It is discouraged to use text messaging for District business. If texting is used for District business, it is recommended that its use be limited to those for whom it is truly necessary (e.g., for specified emergency management functions). All texts created related to District business must be retained by the person creating the text and held in accordance with the Retention Schedule.

### A.22.10 Destruction of Public Records

The District has retained the services of Iron Mountain to act as its document destruction service. All documents and records which have met the Retention Schedule for destruction shall be logged in the Records Destruction log, placed in the locked shredding bins, and taken offsite to their facility for destruction. The certificate of destruction will then be emailed to the Public Records Officer who will place the certificate in the Records Destruction log.

## A.23 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT – HIPAA

### A.23.1 General Security of Electronic and Other Patient and Business Information

San Juan County Public Hospital District No. 1 is committed to providing all aspects of our District and in conducting our business operations in compliance with all applicable laws and regulations. This policy sets forth our commitment for compliance with those standards established by the Department of Health and Human Districts under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the use and disclosure of Protected Health Information ("PHI") under the Privacy Regulations ("Privacy Rule") and the security of Electronic Protected Health Information ("e-PHI") under the Security Regulations (the "Security Rule").

This policy and our procedures as to the creation, use, disclosure, and security of PHI and e-PHI also applies to other essential patient information, billing and business information, and confidential information that is stored electronically or in any other manner, including paper or hard copy form.

**A.23.2 Scope and Applicability**

This policy applies to all the District's members -- including all employees, volunteers, students and trainees (collectively referred to as "staff members") who create, receive or use PHI and e-PHI, and any other confidential patient or business information. It is intended to cover all information system hardware, software and operational procedures. It applies to staff members who may learn of patient information indirectly, and even if use of this information is not part of the staff member's responsibilities.

This Policy addresses our general approach to compliance with the Security Rule. As a covered entity under the Security Rule, the District is required to:

1. Ensure the confidentiality, integrity and availability of all PHI and e-PHI that the District creates, receives, maintains or transmits;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and
4. Ensure compliance with the Privacy and Security Rule by our staff.

Compliance with the Privacy and Security Rules will require the District to implement:

- **Administrative Safeguards--**actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect PHI and e-PHI and to manage the conduct of our staff in relation to the protection of and authorized access to patient information.
- **Physical Safeguards**--physical measures, policies and procedures to protect our electronic information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
- **Technical Safeguards**--the technologies and the policies and procedures for its use that protect PHI and e-PHI and control access.

Procedures for "Scope and Applicability"

**Information Security Officer**

The District has designated a Privacy/Information Security Officer to each agency with overall responsibility for the development and implementation of policies that conform to the Privacy Rule ("Privacy Policies") and the Security Rule ("Security Policies").

The Information Security Officer is responsible for ensuring that the District: (i) complies with the HIPAA Security Policies, (ii) develops and implements HIPAA security procedures ("Security Procedures") for each Security Policy, (iii) maintains the confidentiality of all e-PHI created or received by the District (as well as other essential patient information, billing

and business information, and confidential information that is stored electronically) from the date the information is created or received until it is destroyed, and (iv) trains all staff members of the District at the appropriate level of HIPAA training as determined by the Information Security Officer and Privacy Officer.

**Implementation of Security Measures**

The District will implement any security measure that allows it to reasonably and appropriately comply with a specific security standard in the Security Rule. In determining which security measures to implement, the District will take into account its size, complexity and capabilities; technical infrastructure; hardware and software security capabilities; the costs of the security measures; and the probability and criticality of potential risks to e-PHI.

The District will determine what security measures *must* be implemented and will determine those measures that we have *discretion* to implement. The determination as to what security measures are required or discretionary will be reviewed by the Privacy/Information Security Officer to ensure compliance with the Security Rule.

**Security Complaints**

The Information Security Officer shall be responsible for facilitating a process of individuals (including staff members) to file a complaint regarding our Security Policies or the manner in which e-PHI and other confidential information is handled. The Information Security Officer is responsible for ensuring that the complaint and its disposition are appropriately documented and handled.

**Security Incidents**

It is the responsibility of the Information Security Officer to handle security incidents in collaboration with the District's IT contractor, NWT.

A "Security Incident" is an attempted entry, unauthorized entry, or an information breach or attack on our electronic information system. It includes unauthorized probing and browsing of the files, a disruption of District from any cause, and incidents where electronic information has been altered or destroyed. Security incidents may include such things as a virus or a worm, or unauthorized use of computer accounts and computer systems. It may also include complaints or reports of improper use of our information system.

The Privacy/Information Security Officer is responsible for the following:

- Initiating the appropriate incident management action, including restoration as defined in the Incident Management Procedures.
- Determining the physical and electronic evidence to be gathered as part of the incident investigation.
- Monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- Determining if a widespread communication is required, the content of the communication, and how best to distribute the communication.

- Communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- Initiating, completing, and documenting the incident investigation.

**Mitigation, Sanctions and Non-Retaliation**

The District will ensure it mitigates damages that may occur as a result of any violation of the Security Rule or our Security Policies or specific Security Procedures.

Any staff members (including volunteers) who violate the Security Rule or the District's policies with respect to e-PHI and other protected and confidential information will be disciplined accordingly. This may include verbal or written counseling, suspension, or even termination, depending upon the seriousness of the infraction.

The District will not intimidate or retaliate against any person for exercising his or her rights under the Security Rule or for reporting any concern, issue or practice that the person believes in good faith to be in violation of the Security Rule or our Security Policies or specific Security Procedures.

The District will not require any person to inappropriately waive any rights that person may have to file a complaint with the Department of Health and Human Districts.

**Security Policies and Procedures**

The District's Security Policies and Security Procedures are designed to ensure compliance with the Security Rule. These Security Policies and Security Procedures will be kept current and in compliance with any changes in the law or regulations. There will be periodic evaluation of our Security Policies and Procedures whenever there are significant changes in the law or regulations or at least on an annual basis when there are no such changes.

**Responsibility of All Staff Members**

The District takes privacy issues very seriously, especially in light of the work that we do in healthcare. We will only recruit, hire, or accept staff members who are sensitive to patient privacy and who demonstrate a commitment to the principles of protecting our patient information and our business and other confidential information.

Every member of the District staff is responsible for being aware of, and complying with, the Privacy Rule, the Security Rule, and our Privacy and Security Policies and Procedures. This is an essential requirement of all positions within the organization.

All staff members are responsible for immediately reporting a security incident or suspected security incident immediately.

**Supervision of Staff Members Who Work With e-PHI**

All staff members who use, access or work with e-PHI shall be supervised by appropriate members of management in accordance with their level of e-PHI access. For instance, the use of e-PHI by staff members in the billing department will be supervised by the billing department manager or other appropriate member of management who oversees that

function. The use of e-PHI by field providers will be supervised by the appropriate field/operations supervisory personnel and/or line officers as appropriate.

### A.23.3 Information Security Risk Assessment and Analysis

The District is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The foundation of compliance with the Security Rule is the completion of a "Risk Assessment" to identify existing and potential flaws in the security of our electronic information system, and the related computer systems that are part of it. This policy describes our general approach to Risk Assessment under the Security Rule.

Procedures for "Information Security Risk Assessment and Analysis"

The Privacy/Information Security Officer will develop and implement a documented risk assessment procedure. This procedure will form the basis for identifying all critical information system assets and resources, and to evaluate the potential security problems that may occur.

The District's management personnel and the Privacy/Information Security Officer will undertake a risk analysis process that includes the following:

- Determine and identify the sources of e-PHI within the organization and the manner in which it is stored and transmitted.
- Determine the type of and degree of threats or potential threats to the information system where e-PHI is stored and utilized.
- Identify all potential vulnerabilities to the information system.
- Evaluate the likelihood of risk occurrence (all potential and actual threats to e-PHI will be identified and logged).
- Determine the impact that risks and vulnerabilities to those risks may have on the information system.
- Determine changes that need to be made to minimize the impact of all risks and vulnerabilities to the information system and the cost of those changes.
- Provide recommendations to improve and control the security of the information system.
- If the encryption and decryption of the information should be implemented based on the type of information, its destination (internal or external) and the risk of improper interception

The Risk Assessment will be evaluated against the cost of implementation of each of the recommendations.

Implementation specifications under the Security Rule that are "required" must be implemented and documented that they were in fact implemented, including how the specification was implemented.

Implementation specifications under the Security Rule that are "addressable" will be implemented as follows. The assessment of the addressable standards will be periodically reviewed and assessed:

- If the implementation specification is reasonable and appropriate, The District will implement it.
- If the implementation specification is determined to be inappropriate and/or unreasonable, but the security standard cannot be met without implementation of an additional security safeguard, the District may implement an alternative measure that achieves the addressable specification.
- If the District meets the standard through alternative measures, the decision not to implement the specification will be documented, including the reason for the decision, the rationale, and a description of the alternative safeguard that was implemented.

**A.23.4 Commitment to Protecting the Privacy and Security of Patient Information**

The District is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

A cornerstone of compliance with these regulations is to conduct both a "Gap Analysis" to review and determine where compliance efforts must be focused under the Privacy Rule, and a "Risk Assessment" to identify threats and potential threats to the security of our electronic information system and computer network. This includes ensuring the confidentiality, availability and integrity of protected health information (PHI) stored in non-electronic formats such as paper, and electronic protected health information (e-PHI), the health information stored in our computer system.

This policy provides an overview of our compliance activities in these two important areas of privacy protection for our patients, and identifies our commitment to following industry "best practices" in all areas of compliance with the privacy regulations.

Procedures for "Commitment to Protecting the Privacy and Security of Patient Information"

**Privacy "Gap" Analysis**

- The Privacy Officer will perform a Privacy Gap Analysis utilizing the Privacy Gap Analysis Tool
- The Privacy Officer will report the results of the Privacy Gap Analysis to management
- Management will implement the appropriate forms, policies, procedures, training, etc. necessary to implement the required privacy measures.

**Security Risk Assessment**

- The Information Security Officer will perform a Security Risk Assessment utilizing the Security Risk Assessment Tool.
- The Information Security Officer will report the results of the Security Risk Assessment to management.
- Management will implement the appropriate forms, policies, procedures, training, etc. necessary to implement the required security measures.

### A.23.5 Patient Access, Amendment and Restriction on Use of PHI

Under the HIPAA Privacy Rule, individuals have the right to access and to request amendment or restriction on the use of their protected health information, or PHI, and restrictions on its use that is maintained in "designated record sets," or DRS. (See policy on Designated Record Sets.)

To ensure that the District only releases the PHI that is covered under the Privacy Rule, this policy outlines procedures for requests for patient access, amendment, and restriction on the use of PHI.

This policy also establishes the procedure by which patients or appropriate requestors may access PHI, request amendment to PHI, and request a restriction on the use of PHI.

Procedures for "Patient Access, Amendment and Restriction on Use of PHI"

Only information contained in the designated Record sets (DRS) outlined in this policy is to be provided to patients who request access, amendment and restriction on the use of their PHI in accordance with the Privacy Rule and the Privacy Practices of the District.

**Patient Access**

1. Upon presentation to the business office, the patient or appropriate representative will complete a Request for Access Form.
2. The District staff member must verify the patient's identity, and if the requestor is not the patient, the name of the individual and reason that the request is being made by this individual. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose.
3. The completed form will be presented to the Privacy Officer for action.
4. The Privacy Officer will act upon the request within 30 days, preferably sooner. Generally, the District must respond to requests for access to PHI within 30 days of receipt of the access request, unless the designated record set is not maintained on site, in which case the response period may be extended to 60 days.
5. If the District is unable to respond to the request within these time frames, the requestor must be given a written notice no later than the initial due date for a response, explaining why the District could not respond within the time frame, and in that case the District may extend the response time by an additional 30 days.
6. Upon approval of access, the patient will have the right to access the PHI contained in the DRS outlined below and may make a copy of the PHI contained in the DRS upon verbal or written request.
7. The business office will establish a reasonable charge for copying PHI for the patient or appropriate representative.
8. Patient access may be denied for the reasons listed below, and in some cases the denial of access may be appealed to the District for review.
9. The following reasons to deny access to PHI are not subject to review and are final and may not be appealed by the patient:
    a. If the information the patient requested was compiled in reasonable anticipation of, or use in, a civil, criminal or administrative action or proceeding;
    b. If the information the patient requested was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

10. The following reasons to deny access to PHI are subject to review and the patient may appeal the denial:
    a. If a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
    b. If the protected health information makes reference to another person (other than a health care provider) and a licensed health professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that person;
    c. If the request for access is made by a requestor as a personal representative of the individual about whom the requestor is requesting the information, and a licensed health professional has determined, in the exercise of professional judgment, that access by you is reasonably likely to cause harm to the individual or another person.
    d. If the denial of the request for access to PHI is for reasons a, b, or c, then the patient may request a review of the denial of access by sending a written request to the Privacy Officer.
    e. The District will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny the patient access. The District will promptly refer the request to this designated review official. The review official will determine within a reasonable period of time whether the denial is appropriate. The District will provide the patient with written notice of the determination of the designated reviewing official.
    f. The patient may also file a complaint in accordance with the Procedure for Filing Complaints About Privacy Practices if the patient is not satisfied with the District's determination.
11. Access to the actual files or computers that contain the DRS that may be accessed by the patient or requestor should not be permitted. Rather, copies of the records should be provided for the patient or requestor to view in a confidential area under the direct supervision of a designated District staff member. UNDER NO CIRCUMSTANCES SHOULD ORIGINALS OF PHI LEAVE THE PREMISES.
12. If the patient or requestor would like to retain copies of the DRS provided, then the District may charge a reasonable fee for the cost of reproduction.
13. Whenever a patient or requestor accesses a DRS, a note should be maintained in a log book indicating the time and date of the request, the date access was provided, what specific records were provided for review, and what copies were left with the patient or requestor.
14. Following a request for access to PHI, a patient or requestor may request an amendment to his or her PHI, and request restriction on its use in some circumstances.

**Requests for Amendment to PHI**

1. The patient or appropriate requestor may only request amendment to PHI contained in the DRS. The "Request for Amendment of PHI" Form must be accompanied with any request for amendment.
2. The District must act upon a Request for Amendment within 60 days of the request. If the District is unable to act upon the request within 60 days, it must provide the

requestor with a written statement of the reasons for the delay, and in that case may extend the time period in which to comply by an additional 30 days.

**Granting Requests for Amendment**

1. All requests for amendment must be forwarded immediately to the Privacy Officer for review.
2. If the Privacy Officer grants the request for amendment, then the requestor will receive a letter indicating that the appropriate amendment to the PHI or record that was the subject of the request has been made.
3. There must be written permission provided by the patient so that the District may notify the persons with which the amendments need to be shared. The District must provide the amended information to those individuals identified as having received the PHI that has been amended, as well as those persons or business associates that have such information and who may have relied on or could be reasonably expected to rely on the amended PHI.
4. The patient must identify individuals who may need the amended PHI and sign the statement in the Request for Amendment form giving the District permission to provide them with the updated PHI.
5. The District will add the request for amendment, the denial or granting of the request, as well as any statement of disagreement by the patient and any rebuttal statement by the District to the designated record set.

**Denial of Requests for Amendment**

1. The District may deny a request to amend PHI for the following reasons: 1) If the District did not create the PHI at issue; 2) if the information is not part of the DRS; or 3) the information is accurate and complete.
2. The District must provide a written denial, and the denial must be written in plain language and state the reason for the denial; the individual's right to submit a statement disagreeing with the denial and how the individual may file such a statement; a statement that, if the individual does not submit a statement of disagreement, the individual may request that the provider provide the request for amendment and the denial with any future disclosures of the PHI; and a description of how the individual may file a complaint with the covered entity, including the name and telephone number of an appropriate contact person, or to the Secretary of Health and Human Districts.
3. A statement will be given to that individual that he/she may, if they do not wish to submit a statement of disagreement, request that the Request for Amendment and the denial become a permanent part of their medical record; and
4. A statement will be given to that individual that he/she may complain to the Privacy Officer of the District by marking envelope "Privacy Officer" and sending it to PO Box 370 Friday Harbor, WA 98250, or to the federal agency that oversees enforcement of the federal Privacy Rule, the Department of Health and Human Districts.
5. If the individual submits a "statement of disagreement," the provider may prepare a written rebuttal statement to the patient's statement of disagreement. The statement of disagreement will be appended to the PHI, or at the District's option, a summary of the disagreement will be appended, along with the rebuttal statement of the District.

6. If the District receives a notice from another covered entity, such as a hospital, that it has amended its own PHI in relation to a particular patient, the ambulance District must amend its own PHI that may be affected by the amendments.

**Requests for Restriction**

1. The patient may request a restriction on the use and disclosure of their PHI.
2. The District is not required to agree to any restriction, and given the emergent nature of our operation, we generally will not agree to a restriction.
3. ALL REQUESTS FOR RESTRICTION ON USE AND DISCLOSURE OF PHI MUST BE SUBMITTED IN WRITING ON THE APPROVED DISTRICT FORM. ALL REQUESTS WILL BE REVIEWED AND DENIED OR APPROVED BY THE PRIVACY OFFICER.
4. If the District agrees to a restriction, we may not use or disclose PHI in violation of the agreed upon restriction, except that if the individual who requested the restriction is in need of emergency services, and the restricted PHI is needed to provide the emergency services, the District may use the restricted PHI or may disclose such PHI to another health care provider to provide treatment to the individual.
5. The agreement to restrict PHI will be documented to ensure that the restriction is followed.
6. A restriction may be terminated if the individual agrees to or requests the termination. Oral agreements to terminate restrictions must be documented. A current restriction may also be terminated by the District, as long as the District notifies the patient that PHI created or received after the restriction is removed is no longer restricted. PHI that was restricted prior to the District voiding the restriction must continue to be treated as restricted PHI.

### A.23.6 Privacy and Information Security Training

All members of the District who have access to patient information should understand the organization's concern for the respect of patient privacy and be trained in the District's policies and procedures regarding Protected Health Information (PHI) and the security of e-PHI.

Procedures for "Privacy and Information Security Training"

1. All current staff will be required to undergo privacy and security training in accordance with the HIPAA Privacy Rule and the HIPAA Security Rule. (Security training must occur before April 20, 2011.)
2. All new staff members will be required to undergo privacy training in accordance with the HIPAA Privacy and Security Rules within a reasonable time upon association with the organization, as scheduled by the Privacy/Information Security Officer.
3. All staff members will be required to undergo privacy training in accordance with the HIPAA Privacy and Security Rules within a reasonable time after there is a material change to the District's policies and procedures on privacy practices and the security of patient information.
4. The Privacy and Security Training will be conducted by the Privacy/Information Security Officer or his or her designee.
5. All attendees will receive copies of the District's policies and procedures regarding privacy and security of e-PHI.

6. All attendees must personally complete the training and verify completion and agreement to adhere to the District's policies and procedures on privacy and security practices.
7. Training will be conducted in the following manner:
8. All staff and volunteers will receive annual Privacy and Security Training. Methods used include video tapes, classroom and computer generated instruction and testing of comprehension of material.
9. Topics of the training will include a complete review of the District's privacy and security policies and procedures and will include other information concerning the HIPAA Privacy and Security Rules, such as, but not limited to, the following topic areas:
    a. Overview of the federal and state laws concerning patient privacy including the Privacy and Security Regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    b. Description of protected health information (PHI) and electronic protected health information (e-PHI)
    c. Patient rights under the HIPAA Privacy Rule
    d. Staff member responsibilities under the Privacy and Security Rules
    e. Role of the Privacy/Information Security Officer and reporting employee and patient concerns regarding privacy issues
    f. Importance of and benefits of privacy compliance
    g. Consequences of failure to follow established privacy and security policies
    h. Use of the District's specific privacy and security forms

**A.23.7 Assignment of Responsibilities: The Privacy and Information Security Officers**

The District is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Both privacy and security compliance under HIPAA are very important responsibilities. The District will assign the responsibility of Privacy Officer and Information Security Officer to a staff member knowledgeable about the Privacy and Security Rules, and who will be able to devote the time and energy to the important responsibilities that come with this assignment.

The Privacy Officer and Information Security Officer are high level positions in the organization and as such, the persons assigned to these responsibilities will have access to the highest levels of management to review and discuss policies and procedures, as well as compliance issues and concerns related to the HIPAA Privacy and Security Regulations.

The Privacy Officer and the Information Security Officer may be the same person, since the privacy-related responsibilities between the Privacy Rule and the Security Rule are similar in many respects. The District may also break out the privacy and security compliance responsibilities into two separate positions, depending on workload and organizational need. The Privacy and Information Security Officers may delegate appropriate duties to other responsible staff members.

<u>Procedures for "Assignment of Responsibilities: The Privacy and Information Security Officers"</u>

The following is an overview of the compliance responsibilities of both functions:

**Privacy Officer Responsibilities**

The Privacy Officer oversees all activities related to the development, implementation, and maintenance of the District's policies and procedures covering the privacy of patient health information. This person serves as the key compliance officer for all federal and state laws that apply to the privacy of patient information, including the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Privacy Regulations under that law.

- This individual is tasked with the responsibility of ensuring that all of the organization's patient information privacy policies and procedures related to the privacy of, and access to, patient health information are followed.
- Develops policies and procedures on staff training related to the privacy of patient health information and protected health information.
- Defines levels of staff access to PHI and minimum necessary requirement for staff based on the required job responsibilities.
- Oversees, directs, delivers, and ensures the delivery of initial and ongoing privacy training and orientation to all staff members, employees, volunteers, students and trainees.
- Serves as the contact person for the dissemination of PHI to other health care providers.
- Serves as the contact person for patient complaints and requests.
- Processes patient requests for access to and amendment of health information and consent forms.
- Processes all patient accounting requests.
- Ensures the capture and storage of patient PHI for the minimum period required by law.
- Ensures ambulance District compliance with all applicable Privacy Rule requirements and works with legal counsel and other managers to ensure the District maintains appropriate privacy and confidentiality notices and forms and materials.
- Cooperates with the state and federal government agencies charged with compliance reviews, audits and investigations related to the privacy of patient information.

**Information Security Officer Responsibilities**

The Information Security Officer oversees all activities related to the development, implementation, and maintenance of the District's policies and procedures covering the security of electronic patient health information (e-PHI). This person serves as the key compliance officer for all federal and state laws that apply to the security of patient information, including the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Security Regulations under that law.

This individual is tasked with the responsibility of ensuring that all of the organization's patient information privacy policies and procedures related to the privacy of, and access to, patient health information are followed:

- Ensures that the necessary and appropriate HIPAA related policies are developed and implemented to ensure the security and integrity of all e-PHI within our District and as provided to our business associates.

- Ensures that the necessary infrastructure of personnel, procedures and systems is in place to develop and implement the necessary HIPAA- related policies with respect to the security of e-PHI.
- Ensures that the necessary infrastructure of personnel, procedures and systems is in place to assess, analyze, monitor, and review the District's compliance with all HIPAA-related security policies.
- Develops policies on the security of health care information, including computer and password security and patient data integrity.
- Ensures that the necessary infrastructure of personnel, procedures and systems is in place to provide a mechanism for reporting security incidents and HIPAA security violations.
- Acts as a spokesperson and single point of contact for the District in all issues related to HIPAA security.
- Periodically reviews all security policies to ensure that they maintain their viability and effectiveness.
- Develops and conducts educational programs for District staff to help ensure their compliance with all e-PHI policies and procedures.
- Cooperates with the state and federal government agencies charged with compliance reviews, audits and investigations related to the security of patient information.
- Manage the appropriate Encryption and decryption of PHI and e-PHI

**A.23.8 Contracting with Business Associates**

The District is responsible for ensuring the security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

An important aspect of protecting this information is to ensure that those persons and entities we trust to use patient information on our behalf protect it as we would. This policy describes our approach to entering into agreements with persons and organizations outside of the District, who perform services on our behalf. They must be required, under penalty of termination of the agreement, to abide by all privacy and security regulations.

Procedures for "Contracting with Business Associates"

- The District will identify persons and organizations that perform Districts on our behalf and who in any manner use or story confidential and protected health information about our patients.
- All such persons are called "business associates" (BAs) of San Juan County Public Hospital District No. 1, and they must agree to our privacy and security of information procedures and requirements if they wish to do business with us.
- All managers are required to identify business associates in their respective areas, and report them to the Privacy Officer.
- The Privacy Officer will maintain a current list of business associates.
- All contracts and agreements between the District and any contractor that may come into contact with PHI that we create, use or store in any manner to ensure that business associate language and protections are included in the contract terms.

- Managers must ensure that in any agreements with a business associate where there is a BA agreement separate from the main agreement that the main agreement specifically refers to the BA agreement.
- All managers must ensure that, in any relationship with a vendor that is identified as a business associate (even those where there is no written contract), a written business associate agreement is signed.
- No disclosures of PHI or e-PHI will be made by any staff member until it is verified that there is a current BA agreement on file.
- The Privacy Officer will be responsible for maintaining BA agreements on file for periodic review and inspection.

**A.23.9 Evaluating and Updating HIPAA Polices, Procedures and Training**

The District has adopted this policy to ensure that its Privacy and Security Policies, Procedures and Training are up to date and effective in safeguarding the confidentiality, integrity and availability of PHI and e-PHI created, received, maintained and transmitted by San Juan County Public Hospital District No. 1. It is the goal of the District to adjust our policies and procedures accordingly based on periodic reviews and evaluations of our privacy protection systems.

The Privacy/Information Security Officer will have overall responsibility for monitoring all new developments in patient privacy and security of patient information and will recommend updates to the compliance program as necessary

Procedures for "Evaluating and Updating HIPAA Polices, Procedures, and Training"

**Maintaining Knowledge**

1. The Privacy/Information Security Officer will strive to keep current with all changes in the law and regulations that address the privacy and security of patient information.
2. The Privacy/Information Security Officer will subscribe to professional journals and newsletters on the subject of privacy protection, and will sign up for appropriate list-serves to obtain current information.
3. The Privacy/Information Security Officer will monitor Internet sites periodically for new information on compliance issues related to patient privacy.
4. The Privacy/Information Security Officer will attend seminars and conferences on privacy protection as needed and as the budget allows.
5. The Privacy/Information Security Officer will consult with legal counsel as necessary to learn of new legal developments that could affect San Juan Island EMS and MedEvac with respect to privacy issues.

**Evaluation of Policies and Procedures**

1. On at least an annual basis, the Privacy/Information Security Officer will convene a committee of managers and staff members to identify and review all existing policies and procedures for compliance with current law and regulations regarding privacy.
2. Any member of the review committee or any other staff member may suggest changes to our Privacy and Security Policies or Procedures by submitting the suggestion to the Privacy/Information Security Officer for consideration.

3. The annual policy and procedure review will include an identification of all changes that need to be made to our policies, based on the experience of staff and management and changes in the regulatory environment during the prior year.
4. Any critical changes in the law or regulations that require a change in our privacy practices will be addressed immediately and incorporated into our privacy compliance program.
5. All complaints and concerns regarding the safeguarding of patient information will be evaluated by the Privacy/Information Security Officer to determine if policy or procedure changes need to be implemented.
6. Unwritten procedures and practices will also be reviewed to ensure compliance with the Privacy and Security regulations.

**Evaluating and Updating Training Programs**

1. The Privacy/Information Security Officer will be the keeper of all HIPAA-related training materials and will update those materials and keep them current with recent changes in privacy practices as necessary.
2. Additional in-District training will be scheduled as necessary to ensure that all staff members are kept up to date.
3. An updated privacy and security training program will be provided to the staff on an annual basis.
4. New staff members will be provided with updated privacy and security training upon employment and as otherwise necessary.

**Updating Password Assignments**

1. The Privacy/Information Security Officer will monitor the use of passwords to access the electronic information system.
2. On an annual basis, the Privacy/Information Security Officer will update the password assignment policy and recommend any necessary changes.
3. All District staff members will keep, use, protect and change their access passwords in accordance with the procedures communicated by the Privacy/Information Security Officer.
4. All staff members must adhere strictly to the password procedures established by the District.

**Annual Security Assessment**

1. The Privacy/Information Security Officer will develop a process for completing an annual “walk through” of all areas where e-PHI is used, stored, or transmitted.
2. The walk through will be used to identify strengths and weaknesses in our current security compliance program and to make recommended changes to update our process as needed.
3. Physical security changes will be implemented based on the results of this the annual walk through, and through information collected from other sources, such as staff members, other managers, business associates, and patients.

### A.23.10 Workforce Sanction Policy for Violation of Privacy and Security Policies and Procedures

An important aspect of protecting this information is to make it clear to all staff members that the District takes privacy and security issues very seriously. Any breach of our privacy and security policies are very serious. Not only does the law require that we appropriately sanction staff members for privacy violations, our patients and the public expect us to do just that.

This section describes our approach to staff member sanctions when there is a violation of our privacy and security policies.

Any sanctions under this policy or any other policy will not apply to staff members who 1) file a complaint with the federal government about potential privacy violations, 2) testify, assist, or participate in an investigation or compliance review proceeding or official government proceeding investigating privacy issues, and 3) oppose any actions by the District that are unlawful under the HIPAA Privacy Rule or the HIPAA Security Rule, when that opposition is made with the good faith belief that San Juan County Public Hospital District No. 1 was violating privacy or security regulations (as long as any opposition or filing of a complaint did not result in improper disclosure of PHI or e-PHI).

Procedures for "Workforce Sanction Policy for Violation of Privacy and Security Polices and Procedures"

1. The District will implement sanctions that are to be used when any staff member fails to comply with or violates our privacy policies and procedures.
2. Sanctions will be administered in a progressive manner wherever possible. The District will administer sanctions to the degree necessary to correct improper behavior or to protect patient privacy. (EXAMPLE: A first time violation where an employee revealed PHI to another staff member without any need to know may receive a verbal counseling or written warning, but if a first violation of a single patient's PHI resulted in revealing PHI to someone who was not a staff member or business associate, a suspension may be warranted. More substantial breaches may result in termination even on a first-time offense.)
3. Progressive sanctions may include the following:
    a. Remedial training and education
    b. Informal verbal counseling
    c. Formal verbal counseling with written documentation of the counseling
    d. Written warning
    e. Suspension
    f. Termination or expulsion from the District
4. Staff members have an affirmative duty to report to management or the Privacy Officer or Information Security Officer any suspected violation of our privacy/security policies and procedures.
5. Staff members shall be educated about this policy and the serious nature of violating our privacy/security policies. Staff members will be made aware of the potential sanctions that may occur, and will be made aware of any changes to this sanction policy.

6. A record of individual staff member sanctions will be kept in the respective staff member's file. Adherence to our privacy/security polices will be considered as part of the staff member's performance evaluation.
7. In the event of a suspected or reported violation of our privacy/security policies, the Privacy/Information Security Officer will initiate an objective and comprehensive investigation that will include:
    a. Interviews of potential witnesses
    b. Interviews of the alleged violator
    c. Preparation of an investigative report
    d. Presentation of the report to management with recommendations for sanctions (if any) or changes in our policies or practices
8. At all times, whenever there is a suspected violation of our policies or other breach of privacy, the Privacy/Information Security Officer will recommend immediate action to be taken to mitigate the violation and its impact on the District.

**A.23.11 Levels of Access, "Minimum Necessary Standard" and Limiting Disclosure and Use of PHI and e-PHI**

Security of PHI and e-PHI is everyone's responsibility. This section outlines levels of access to Protected Health Information (PHI) and electronic protected health information (e-PHI) of various staff members of the District and provides our policy and general procedures on limiting access, disclosure, and use of PHI.

The District retains strict requirements on the security, access, disclosure and use of PHI and e-PHI. Access, disclosure and use of PHI and e-PHI will be based on the role of the individual staff member in the organization, and should be only to the extent that the person needs access to patient information to complete necessary responsibilities for San Juan County Public Hospital District No. 1.

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

Procedures for "Levels of Access, "Minimum Necessary Standard" and Limiting Disclosure and Use of PHI and e-PHI

**Role Based Access**

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

| Job Title | Description of PHI and e-PHI to Be Accessed | Conditions of Access to PHI and e-PHI |
|---|---|---|
| **EMT** | Intake forms from dispatch, patient care reports | May access only as part of completion of a patient event and post-event activities and only while actually on duty |
| **Paramedic** | Intake forms from dispatch, patient care reports | May access only as part of completion of a patient event and post-event activities and only while actually on duty |
| **Billing Clerk** | Intake forms from dispatch, patient care reports, billing claim forms, remittance advice statements, other patient records from facilities | May access only as part of duties to complete patient billing and follow up and only during actual work shift |
| **Field Supervisor** | Intake forms from dispatch, patient care reports | 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 |
| **Dispatcher** | Intake forms, preplanned CAD information on patient address | May access only as part of completion of an incident, from receipt of information necessary to dispatch a call, to the closing out of the incident and only while on duty |
| **Training Coordinator** | Intake forms from dispatch, patient care 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 |
| **Agency Managers** | | May access only to the extent necessary to monitor compliance and to accomplish appropriate supervision and management of personnel |

Access to PHI and e-PHI is limited to the above-identified persons only, and to the identified patient information only, based on the District's reasonable determination of the persons or classes of persons who require PHI, and the nature of the health information they require, consistent with their job responsibilities.

This does not prevent the release of any patient information among staff members or among staff members and other health care providers necessary to carry out proper treatment and transport of the patient.

Access to a patient's entire file will not be allowed except when provided for in this and other policies and procedures and the justification for use of the entire medical record is specifically identified and documented.

**Disclosures to and Authorizations from the Patient**

Staff are not required to limit to the minimum amount of information necessary required to perform their job function, or disclosures of PHI or e-PHI to patients who are the subject of the information. In addition, disclosures authorized by the patient are exempt from the minimum necessary requirements unless the authorization to disclose PHI or e-PHI is requested by the District.

Authorizations received directly from third parties, such as Medicare or other insurance companies, which direct staff to release PHI or e-PHI to those entities are not subject to the minimum necessary standards.

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

**District Requests for PHI and e-PHI**

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

| Holder of PHI or e-PHI | Purpose of Request | Information Reasonably Necessary to Accomplish Purpose |
|---|---|---|
| **Skilled Nursing Facilities** | To have adequate patient records to determine medical necessity for District and to properly bill for Districts provided | Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments |
| **Hospitals** | To have adequate patient records to determine medical necessity for District and to properly bill for Districts provided | Patient face sheets, discharge summaries, Physician Certification Statements and Statements of Medical Necessity, Mobility Assessments |
| **Mutual Aid Ambulance or Paramedic Districts** | To have adequate patient records to conduct joint billing operations for patients mutually treated/transported by the District | Patient care reports |

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

**Incidental Disclosures**

The District understands that there will be times when there are incidental disclosures about PHI or e-PHI in the context of caring for a patient. The privacy laws were not intended to impede common health care practices that are essential in providing health care to the individual. Incidental disclosures are inevitable, but these will typically occur in radio or face-to-face conversation between health care providers, or when patient care information in written or computer form is left out in the open for others to access or see.

The fundamental principle is that all staff members need to be sensitive about the importance of maintaining the confidence and security of all material we create or use that contains patient care information. Coworkers and other staff members should not have access to information that is not necessary for the staff member to complete his or her job. For example, it is generally not appropriate for field personnel to have access to billing records of the patient.

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

**Verbal Security**

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

Garage Areas: Staff members should be sensitive to the fact that members of the public and other agencies may be present in the garage and other easily accessible areas. Conversations about patients and their health care should not take place in areas where those without a need to know are present.

Other Areas: Staff members should only discuss patient care information with those who are involved in the care of the patient, regardless of your physical location. You should be sensitive to your level of voice and to the fact that others may be in the area when you are speaking. This approach is not meant to impede anyone's ability to speak with other health care providers freely when engaged in the care of the patient. When it comes to treatment of the patient, you should be free to discuss all aspects of the patient's medical condition, treatment provided, and any of their health information you may have in your possession with others involved in the care of the patient.

**Verbal Security**

Patient Care and Other Patient or Billing Records: Patient care reports should be stored in safe and secure areas. When any paper records concerning a patient are completed, they should not be left in open bins or on desktops or other surfaces. Only those with a need to have the information for the completion of their job duties should have access to any paper records.

Billing records, including all notes, remittance advices, charge slips or claim forms should not be left out in the open and should be stored in files or boxes that are secure and in an area with access limited to those who need access to the information for the completion of their job duties.

Computers and Entry Devices: Computer access terminals and other remote entry devices such as PDAs and laptops should be kept secure. Access to any computer device should be by password only. Staff members should be sensitive to who may be in viewing range of the monitor screen and take simple steps to shield viewing of the screen by unauthorized persons. All remote devices such as laptops and PDAs should remain in the physical possession of the individually to whom it is assigned at all times.

### A.23.12 Designated Records Sets

To ensure that the District releases Protected Health Information (PHI) in accordance with the Privacy Rule, this policy establishes a definition of what information should be accessible to patients as part of the Designated Record Sets (DRS), and outlines procedures for requests for patient access, amendment, and restriction on the use of PHI.

Under the Privacy Rule, the DRS includes medical records that are created or used by the District to make decisions about the patient. All staff members should be familiar with the information from the medical records that may be accessible to our patients.

Procedures for "Designated Records Sets"

The DRS should only include HIPAA covered PHI, and should not include information used for the operational purposes of the organization, such as quality assurance data, accident reports, and incident reports. The type of information that should be included in the DRS is medical records and billing records.

The DRS for any requests for access to PHI includes the following records:

- The patient care report or PCR created by EMS field personnel (this includes any photographs, monitor strips, Physician Certification Statements, Refusal of Care forms, or other source data that is incorporated and/or attached to the PCR.
- The electronic claims records or other paper records of submission of actual claims to Medicare or other insurance companies.
- Any patient-specific claim information, including responses from insurance payers, such as remittance advice statements, Explanation of Medicare Benefits (EOMBs), charge screens, patient account statements, and signature authorization and agreement to pay documents.

- Medicare Advance Beneficiary Notices, Notices from insurance companies indicating coverage determinations, documentation submitted by the patient, and copies of the patient's insurance card or policy coverage summary, that relate directly to the care of the patient.
- Amendments to PHI, or statements of disagreement by the patient requesting the amendment when PHI is not amended upon request, or an accurate summary of the statement of disagreement.

The DRS should also include copies of records created by other District providers and other health care providers such as first responder units, assisting ambulance Districts, air medical Districts, nursing homes, hospitals, police departments, coroner's office, etc., that are used by the District as part of treatment and payment purposes related to the patient.

**A.23.13 News Media Interaction Policy**

This policy is necessary as federal law protects a patient's general right to privacy under the Privacy Regulations of the Health Insurance Portability and Accountability Act (HIPAA). State law protections from invasion of privacy may also apply.

As a general rule, since the District is covered by HIPAA, we may not release PHI to anyone, absent a patient's written authorization, except for purposes of patient treatment, billing or other health care operations related to the District. The District may release certain information as long as the information is "de-identified," meaning that the person who receives the information would not likely be able to ascertain the identity of the patient with the information we provide, or if permission is given by the patient.

The District must balance providing the public with information about the Districts we provide against the individual rights of the patient to keep their medical information confidential. We fully respect the right of the public to know about our activities as we are a public agency subject to public scrutiny. But we can provide information to the public only to the extent that the law allows us.

We will at all times treat members of the media in a professional manner when a request for information is made.

Procedures for "News Media Interaction Policy"

All requests for information from the news media shall be directed to the Public Information Officer or the Superintendent. Staff members are not permitted to release information to the news media, including patient records or reports at any time except as authorized by a supervisor.

The District maintains the highest standards of patient confidentiality. It is impossible, however, to accomplish this standard without the compliance of our staff. To ensure that there are no inappropriate disclosures or uses of a patient's PHI, only the following information may be disclosed by the District to members of the media as follows:

- **Name of Hospital.** You may provide the name of the hospital to which patients have been transported. (Acceptable Example: The media calls about "the accident at Third

and Main earlier this afternoon." You may inform the media "a patient was transported from the accident scene to St. Joseph's Medical Center in Bellingham."). THE NAME OF THE PATIENT SHOULD NOT BE RELEASED TO THE MEDIA. It is not appropriate for us to confirm or deny the identity of a patient. Requests for patient identity should be directed to a law enforcement agency or to the hospital. Law enforcement agencies are not subject to the strict requirements of protecting patient information as we are under HIPAA.

- **Number of Patients.** You may provide the total number of patients involved in an accident or transported to a facility. You may not indicate specifics about the vehicle a patient was driving or which patient went to a particular facility. (Acceptable Example: You may inform the media that "four patients were transported from the fire at the Acme Chemical Factory. Two were taken to County General and two were taken to the Regional Medical Center.")
- **Age and Gender.** You may provide the age of a patient and the gender of the patient, unless it could reasonably be used to identify the patient. (Acceptable Example: You may inform the media "a 39 y/o male was transported from the accident on the Interstate." You would not want to disclose to the media "a 39 y/o male was transported from 124 Main St.")
- **Designation of Crew Members.** The designation of crew members as paramedics or EMTs is not protected health information. You may state, for example, that one paramedic and two EMTs were involved in caring for the patients involved in a motor vehicle accident. (You could identify the names of the personnel who responded, but some Districts prefer not to release this information). You are not permitted to describe the specific type of care rendered to patients at the scene or on the way to the hospital. Nor may you speculate on what injuries a patient may or may not have sustained. (Acceptable Example: San Juan Island EMS personnel on the scene of the incident included two paramedics and a supervisor and advanced life support was administered.")
- **Type of Transport.** You may indicate that a particular call was an emergency and that transportation was facilitated by ambulance or helicopter. Do not speculate on the patient's condition even if you are sure of that condition. For example, do not disclose to a member of the media that a patient was critical or stable unless you are comfortable in knowing this to be their general condition. (Acceptable Example: "Of the 3 patients on the scene of the incident, one was transported by helicopter to the SAN JUAN ISLAND EMS AND MEDEVAC Trauma Center and two were transported as non-emergency patients to the local hospital emergency department.")
- **Non-PHI.** Information that is not classified as PHI may be released to the media consistent with District policy and state law. For instance, information about a fire response or a standby that did not involve patient care may be released to the media, as may general information about an event. (Acceptable Example: "We treated 45 patients during the two-day festival, and 6 were transported to local hospitals for various heat-related complaints").
- **Disclosures Authorized by the Patient.** In the event that the patient or the patient's legally responsible decision maker signs a HIPAA authorization form, disclosures of information, including PHI, may be made so long as they are done in accordance with the express terms of the written authorization. Authorization forms for this purpose must be HIPAA-compliant and must be approved by the Privacy Officer.

If at any time you are unclear about whether information may be disclosed to the media, always err on the side of caution and do not disclose the questionable item of information. Again, all requests for patient information should be directed to the Public Information Officer.

**A.23.14 Release of Protected Health Information to Law Enforcement**

The goal of this section is to provide consistent guidelines for District personnel on when they may be permitted to disclose patient information to law enforcement.

Protected health information, or PHI, is defined as individually identifiable health information, created or received by us, that relates to the past, present, or future physical or mental health of a patient, the provision of health care to the patient, or payment for the provision of health care to the patient.

PHI can be in any form including paper, electronic (e-PHI), or verbal. Typical examples of sources where PHI may be contained include PCRs, billing forms, and verbal information about a patient exchanged with others.

There are six (6) specific situations where some or all of a patient's protected health information (PHI) may be disclosed to law enforcement personnel. These situations fall into three (3) general categories:

- Disclosures required by law;
- Disclosures permitted by law; and
- Optional disclosures.

Procedures for "Release of Protected Health Information to Law Enforcement"

The District is required by law to give a patient's PHI to law enforcement regardless of the patient's consent when law enforcement personnel present you with:

- A subpoena, summons, or warrant ("SSW")
- An administrative request/investigative demand
- A request for information pertaining to a limited number of injuries that you must disclose by law

**Subpoena, Summons or Warrant (Required Disclosure)**

Confirm that the paper received is, in fact, a subpoena, summons or warrant and that it specifically identifies the PHI the District is required to disclose. The Privacy Officer is the appropriate person to handle these requests.

A subpoena, summons or warrant is issued by a Court, judicial officer or grand jury. Be sure that the SSW has one of these designations as the issuer. Be sure that the original subpoena is enclosed with the request. References to a subpoena in the request letter are not actionable. You must receive the actual subpoena along with the request letter.

Verify that all written assurances have been made by the requestor. These assurances include that:

- Reasonable efforts have been made by the requestor to notify the individual who is the subject of the requested PHI;
- Reasonable efforts have been made by the requestor to secure a protective order (i.e. an order of the court, an administrative tribunal or a stipulation by the parties to the litigation) that:
    - Prohibits the parties from using or disclosing PHI for any purpose other than the litigation or proceeding for which the PHI was requested; and
    - Requires all PHI (including all copies made) to be returned to the District or destroyed at the end of the litigation or proceeding.

If all written assurances have not been made, send the requestor the form letter stating that the District will not disclose any PHI or e-PHI until the proper written assurances have been made. (Note: This letter is currently formatted to send to an attorney as this will often be the case.)

If all written assurances have been made, send PHI as requested in the subpoena. ONLY send the PHI that has been requested. Do not send the entire patient file if it has not been specifically requested in the subpoena.

**Patient care reports (PCRs)**

The District may or may not be able to just turn over a copy of your PCR to law enforcement. If the SSW is valid, provide ONLY the PHI requested. The District is legally required to disclose ONLY that information that is contained in the four corners of the paper you are given by law enforcement. You are not to disclose any other information not specifically requested.

If the SSW requests the entire PCR, or utilizes language such as "any and all records" pertaining to the patient, the District must provide the entire PCR in response.

Do NOT disclose information based on a verbal request from law enforcement (see Permitted Disclosures and Optional Disclosures procedures below for exceptions).

Keep a copy of the SSW.

Please note: This section addresses SSWs issued by a judicial officer or a grand jury and served by law enforcement, not served by private litigants.'

**Administrative Request/Investigative Demand (Required Disclosure)**

An administrative request/investigative demand is a request for PHI by a federal/state/local government agency authorized to make such requests. The Privacy Officer is the appropriate person to handle these requests.

If the District receives an administrative request/investigative demand, the District may ONLY give out a patient's PHI as long as the information requested is:

- Relevant and material to law enforcement's inquiry,
- Specific and limited in scope to the inquiry, and
- Information (other than PHI) could not be used.

The District should obtain assurances of the above three items from the agency making the investigative demand.

**Burns, Firearm Injuries, Animal Bites, Abuse, Domestic Violence (Required Disclosure)**

EMS providers are, in some states, legally obligated to report to law enforcement certain types of injuries like a gunshot wound, animal bites, burn or incidents of abuse (i.e., child abuse, elder abuse or domestic violence). State law governs these reporting requirements, and these types of disclosures of PHI are permitted where you are required to make such reports under state law. Contact your Supervisor for a list of those injuries that you must report under state law in the particular jurisdiction where you are employed.

**Permitted Disclosures**

Here is a list of the approved situations where PHI may be disclosed, without the patient's authorization, consent or permission, when law enforcement requests PHI for the purpose of:

- Identifying or locating a suspect, material witness or missing person;
- Victim of a crime; and
- Abuse, neglect and domestic violence.

Ask law enforcement the purpose of their request before disclosing PHI.

**Identifying or locating a suspect, material witness, or missing person (Permitted Disclosure)**

If law enforcement indicates that they need the PHI to identify or locate a suspect, material witness, or missing person, you may disclose only the PHI listed below:

- Name
- Address
- Date of birth
- Place of birth
- Social Security Number
- Blood type
- Type of injury
- Date of treatment
- Time of treatment
- Description of distinguishing physical characteristics (i.e. weight, hair color, eye color, gender, facial hair, scars and tattoos)

Do NOT give law enforcement any PHI when the sole purpose of the request is to assist law enforcement with their investigation or to help build a case against a suspect unless an appropriate subpoena or warrant is presented. Law enforcement's request must conform to the procedures outlined in this policy.

Do NOT disclose for the purposes of identification or location any PHI related to the patient's:

- DNA or DNA analysis
- Dental records
- Typing, samples or analysis of body fluids or tissue

**Victim of crime (Permitted Disclosure)**

The law allows more latitude when disclosing information to law enforcement authorities when the information is about a victim of a crime. Victims of a crime may include motor accident victims because often a summary or misdemeanor offense is involved, such as when the accident is the result of the driver of another vehicle violating traffic laws. It is not the District's responsibility to make the determination of whether the patient is an actual crime victim, and in many cases the determination that a patient is or may be a crime victim can be inferred from the circumstances and the presence of law enforcement at the scene.

The best approach is ask the patient (if the patient is conscious and alert) if it is acceptable to disclose the PHI to law enforcement. You may disclose PHI about a crime victim to law enforcement if the crime victim consents to the disclosure.

If the patient is temporarily unable to consent, ask law enforcement if they can wait until the patient is able to consent.

If law enforcement cannot wait until the patient is able to consent because to do so would compromise an immediate law enforcement need (e.g., to determine if a crime has occurred or to determine the location of victims who may need to be interviewed later), then the District's staff member may disclose the patient's PHI.

Ask for and obtain law enforcement's assurance that the PHI provided will not be used against the victim and that the information is needed immediately. While these assurances may be given verbally, document that you received them.

**Abuse, neglect and domestic violence (Permitted Disclosure)**

The District is permitted to disclose PHI about a patient whom it believes is a victim of abuse, neglect or domestic violence, where these disclosures are required by state law. Staff should contact their Supervisor or the designated privacy official for guidance regarding these types of disclosures.

If a staff member believes that a patient is a victim of abuse, neglect or domestic violence, the staff member may disclose PHI to a government authority, including Social Districts and law enforcement, provided they also notify their supervisor.

Ask the patient for his/her consent. If the individual agrees to the disclosure of PHI, a staff member may give this information to law enforcement.

- If the patient does not consent or is unable to consent, the District may disclose PHI to law enforcement as required by State law if:
- You believe the disclosure is necessary to prevent serious harm to the patient or other potential victims, or
- The patient is unable to consent due to incapacity,

- Law enforcement assures you the PHI will not be used against the victim, and
- Law enforcement activities would be adversely affected without the PHI.

If PHI is disclosed without the patient's consent or because the patient was unable to consent, the designated privacy official should contact the patient and alert them of the disclosure, unless you believe contacting the patient will only put the patient at greater risk

**Optional Disclosures**

On-scene communications must involve a commonsense approach. Providing law enforcement with basic information about where you are taking a patient and the patient's general condition (critical, serious, minor, etc.) is normally permissible when the event is a motor vehicle accident or other situation where a crime may have occurred.

Requests for patient information that do not occur at the scene of an incident, but come after the call is over, should be directed to your Supervisor or the Privacy Officer.

Remember at all times that, if you see physical evidence of a potential crime (such as drug paraphernalia, strange white powder in a bag, etc.), this evidence normally should be reported and given to law enforcement officials if it is not proper to leave it in the location it was found.

There are several circumstances where staff may disclose information at their option.

- Decedents. You may disclose PHI to law enforcement when you think your patient died as a result of a crime. Limit the PHI to basic facts about the victim and the circumstances of the death. You may disclose PHI to a coroner regardless of the cause of death. [NOTE: Check your state law for specific requirements as to the coroner's authority and procedures the coroner may have to follow.]
- Crime on Premises. You may disclose to law enforcement any PHI you in good faith believe constitutes evidence of a crime committed on your organization's premises. This includes the station house; headquarters; parking lot; the ambulance or engine, etc.
- Reporting crime in an emergency. You may voluntarily offer PHI to law enforcement when you believe it is necessary to alert law enforcement to:
    - The commission of a crime
    - The nature of a crime
    - The location of the crime
    - The location of a crime victim
    - The identity, description, and location of the perpetrator of a crime

**A.23.15 Access to the Information System and e-PHI**

This section is to ensure that all staff members have appropriate access to e-PHI and PHI, and that his or her identity is properly verified before such access can be attempted. This policy also addresses procedures to prevent staff members and former staff members who should not have access to e-PHI and PHI from obtaining it, and for emergency access to the information system.

This section also addresses the steps to be followed to terminate access to e-PHI and PHI when a staff member's authorization to access has ended, such as when employment or membership is terminated.

Procedures for "Access to the Information System and e-PHI"

**Person or Identify Authorization**

To ensure that all individuals or entities that access e-PHI have been appropriately authenticated, the following procedures are established:

- Staff members seeking access to any network, system, or application that contains e-PHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.
- Staff members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and password, smart card, or other authentication information.
- Workforce members are not permitted to allow other persons or entities to use their Unique User ID and password, smart card, or other authentication information.
- A reasonable effort must be made to verify the authenticity of the receiving person or entity prior to transmitting e-PHI.

**Security Unique User Identification**

To uniquely identify and track one user or workforce member from all others, for the purpose of access control to all networks, systems, and applications that contain e-PHI, and the monitoring of access to the aforementioned networks, systems, and applications, the following procedures are established:

- Any staff member or authorized user that requires access to any network, system, or application that access, transmits, receives, or stores e-PHI, must be provided with a Unique User Identification Number.
- When requesting access to any network, system, or application that access, transmits, receives, or stores e-PHI, a staff member or authorized user must supply their previously assigned Unique User Identification in conjunction with a secure password.
- Staff members or authorized users must not allow anyone else to use their Unique User Identification or password.
- Staff members and authorized users must ensure that their User Identification is not documented, written, or otherwise exposed in an insecure manner.
- Staff members and authorized users must take all reasonable steps to ensure that their assigned User Identification is appropriately protected and only used for legitimate access to networks, systems, or applications.
- If a staff member or authorized user believes their User Identification has been comprised, they must report that security incident to the appropriate supervisor or the Information Security Officer.

**Security Password Management**

To ensure that passwords created and used by the District and its staff to access any network, system, or application used to access, transmit, receive, or store e-PHI is properly safeguarded the following procedures are established:

- All staff members who access networks, systems, or applications used to access, transmit, receive, or store e-PHI must be supplied with a Unique User Identification and password to access e-PHI.
- All staff members must supply a password in conjunction with their Unique User Identification to gain access to any application or database system used to create, transmit, receive, or store e-PHI.
- A generic User Identification and password may be utilized for access to shared or common area workstations so long as the login provides no access to e-PHI. An additional Unique User Identification and password must be supplied to access applications and database systems containing e-PHI.
- All passwords used to gain access to any network, system, or application used to access, transmit, receive, or store e-PHI must be of sufficient complexity to ensure that it is not easily guessable.
- Managers of networks, systems, or applications used to access, transmit, receive, or store e-PHI, must ensure that passwords set by staff members meet the minimum level of complexity described in this policy.
- Managers of networks, systems, or applications used to access, transmit, receive, or store e-PHI are responsible for educating staff members about all password related policies and procedures, and any changes to those policies and procedures.
- Password "aging times" (i.e., the period of time a password may be used before it must be changed) may be implemented in a manner commensurate with the criticality and sensitivity of the e-PHI contained within each network, system, application or database.
- Staff members are responsible for the proper use and protection of their passwords and must adhere to the following guidelines:
    - Passwords are only to be used for legitimate access to networks, systems, or applications.
    - Passwords must not be disclosed to other staff members or individuals.
    - Staff members must not allow other staff members or individuals to use their password.
    - Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.

**Security Password Structure**

To ensure that all passwords used to control access to any network, system, application, media or file containing e-PHI are secure and not easily guessed, the following procedures are established:

- Passwords must be a minimum of eight characters in length
- Passwords must incorporate three of the following characteristics:
- Any lower-case letters (a-z)
- Any upper-case letters (A-Z)

- Any numbers (0-9)
- Any punctuation or non-alphanumeric characters found on a standard ASCII keyboard (! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; “ ‘ | \ / ? < > , . ~ ` )
- Passwords must not include easily guessed information such as personal information, names, pets, birth dates, etc.
- Passwords must not be words found in a dictionary.
- If a system does not support the minimum structure and complexity as detailed in this policy, one of the following procedures must be implemented:
    - The password assigned must be adequately complex to ensure that it is not easily guessed. If an alternative password structure must be implemented, the complexity of the chosen alternative must be defined and documented.
    - The current system must be upgraded to support the minimum HIPAA Security Password Structure.
    - All e-PHI must be removed and relocated to a system that supports the minimum HIPAA Security Password Structure.

**Emergency Access to e-PHI and PHI**

To ensure that access to critical e-PHI is maintained during an emergency situation, the following emergency access procedures are established: If a system contains e-PHI used to provide patient treatment, and the denial or strict access to that e-PHI could inhibit or negatively affect patient care, staff members responsible for electronic information systems must ensure that access to that system is made available to any caregiver in case of an emergency.

**Termination of Access**

To ensure that access to the information system and e-PHI is terminated when a staff no longer has authorization for access, the following procedure is established. This procedure also applies to terminations in employment or membership in the organization, retirement, resignation, leave of absence, or transfer to an area in the organization where the staff member is no longer authorized to access the information system.

- All supervisors will immediately notify the Privacy/Information Security Officer or and the information system administrator when a staff member has been separated from District with the District or when the person no longer is permitted access to the system.
- The staff member’s access to the information system will immediately be disabled on the effective date of the separation or, if still on the staff, the effective date when access authorization has ended.
- The staff member will be removed from all information system access lists.
- The staff member will be removed from all user accounts.
- The staff member will turn in all keys, tokens, or access cards that allow access to the information system.
- The “Staff Member Termination Checklist” (Form 34) will be completed by the supervisor the last day of the staff member’s authorized access.

**Encryption and Decryption**

Security involves protection of e-PHI, PHI and other important District information during its transmission and receipt via electronic means such as electronic mail and file, information, or software transfers. Encrypting and decrypting electronic information and files during their "transit" is a technical means of ensuring that if the information or files are intercepted or end up in the wrong hands, they cannot be deciphered or interpreted.

In effect, encryption turns the transmission into unique "gibberish" that transforms the electronic information or files into something that cannot be viewed in their original form unless it is decrypted at the receiving end. It is like attaching a unique "code" to that information so that it can only be accessed by those with the "de-coder."

While the District is not legally required to "encrypt" electronic information or files in most cases, the District is obligated to ensure that e-PHI, PHI, and other important patient or District information does not fall into the wrong hands or is viewed or used by those who should not have access to it. Thus, it is the policy of the District to use encryption or decryption techniques wherever possible when handling PHI and e-PHI.

### A.23.16 Contingency Planning

This section describes the approach to ensuring that our response to an emergency or other occurrence that threatens or damages our computer, electronic, or other information systems is appropriate. This policy provides for the contingencies necessary to protect and preserve that information in accordance with the HIPAA Security Rule and other regulations

This section also covers the procedures for protecting the integrity of PHI and other essential patient information, billing and business information, and confidential information in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains this information is affected, including:

- Applications and data criticality analysis
- Data backup
- Disaster recovery planning
- Emergency mode operation plan

Procedures for "Contingency Planning"

**Applications and Data Criticality Analysis**

Administration will assess the relative criticality of specific applications and data within the District for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.

The assessment of data and application criticality should be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

**Data Backup Plan**

Each functional area of the District (Operations, Billing, Administration) will establish and implement a Data Backup Plan that ensures that each area of the District will create and maintain retrievable exact copies of all PHI and other essential business information that is at a medium to high risk for destruction or disruption.

The Data Backup Plan must apply to all medium and high-risk files, records, images, voice or video files that may contain PHI and other essential business information.

The Data Backup Plan must require that all media used for backing up PHI and other essential business information be stored in a physically secure environment such as a secure, off-site storage facility. Where backup media remains on site, it will be kept in a physically secure location, different from the location of the computer systems have been backed up.

If an off-site storage facility or backup District is used, a written contract or Business Associate Agreement must be used to ensure that the Business Associate will safeguard any PHI and other essential business information in an appropriate manner.

Data backup procedures and contingency plan shall be tested on a periodic basis to ensure that exact copies of PHI and other essential business information can be retrieved and made available whenever it is needed.

Each functional area of the District with medium and high risk PHI must submit its Data Backup Plan to the HIPAA Information Security Officer for approval.

**Disaster Recovery Plan**

To ensure that each functional area of the District can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting information systems containing PHI or other essential business information, each area will establish and implement a Disaster Recovery Plan. The Plan must ensure that each area can restore or recover any loss of this information and the systems needed to make that information available in a timely manner.

The Disaster Recovery Plan will include procedures to restore PHI and other essential business information from data backups in the case of a disaster causing data loss.

The Disaster Recovery Plan will include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.

The Disaster Recovery Plan must be documented and easily available to the necessary personnel at all time, who should be trained to implement the Disaster Recovery Plan.

The disaster recovery procedures outlined in the Disaster Recovery Plan must be tested on a periodic basis to ensure that PHI and other essential business information and the systems needed to make e-PHI available can be fully restored or recovered.

Each functional area at a medium and high risk of compromise of PHI and other essential business information must submit its Disaster Recovery Plan to the HIPAA Information Security Officer for approval.

**Emergency Mode Operation Plan**

Each functional area of the District must establish and implement (as needed) procedures to enable continuation of administrative, patient care, and billing and business processes for protection of the security of PHI and other essential business information while operating in emergency mode. Emergency mode operation procedures outlined in the Emergency Mode Operation Plan must be tested periodically to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode. Each functional area at a medium and high risk of compromise of e-PHI must submit its Emergency Mode Operation Plan to the Information Security Officer for approval.

### A.23.17 Disaster Management and Recovery of e-PHI

This "Disaster Management" section of the District's HIPAA policy will be followed in an emergency situation such as or disaster such as fire, vandalism, terrorism, system failure, or natural disaster.

As a providers of critical healthcare services, it is the District's policy to ensure the District will be able to recover from a serious information system disruption, including situations that could lead to the loss of data in the event of an emergency or disaster (such as fire, vandalism, terrorism, system failure, or natural disaster) and that the following procedures are established to that end.

Procedures for Disaster Management and Recover of e-PHI

**Disaster Recovery Planning**

A disaster recovery plan will be established and implemented to restore or recover any loss of e-PHI and any loss or disruption to the systems required to make e-PHI available.

The disaster recovery plan will be developed by staff members responsible for the maintenance of the security and integrity of the information system and will be reviewed and approved by the Privacy/Information Security Officer and senior management.

- A data backup plan including the storage location of backup media.
- Procedures to restore e-PHI from data backups in the case of an emergency or disaster that results in a loss of critical data.
- Procedures to ensure the continuation of business critical functions and processes for the protection of e-PHI during emergency or disaster situations.
- Procedures to periodically test data backup and disaster recovery plans.
- Procedures to periodically perform an application and data criticality analysis establishing the specific applications and e-PHI that is necessary to maintain operation in an emergency mode.
- Procedures to log system outages, failures, and data loss to critical systems.
- Procedures to train the appropriate personnel to implement the disaster recovery plan.
- The disaster recovery plan must be documented and easily available to the necessary personnel at all times.

**Current Disaster Recovery Plan**

The District backs up all data through the use of NW Tech. This data can easily be restored by authorization of the Agency Head.

- The District should annually check with NW Tech to ensure ongoing storage of key data
- All system errors are reported and tracked by NW Tech

The District makes use of remote login software for all patient records (ESO at San Juan Island EMS, Eldermark at Village at the Harbor). This ensures that data is well backed up.

The largest risk to data is accidental deletion. This risk is mitigated by controlling access to the records.

### A.23.18 Physical Security of PHI and e-PHI

This policy describes our general approach to facility security and the steps necessary to prevent a breach in the physical security system in place. It also describes our general procedures to limit physical access to electronic information systems and the buildings and rooms in which they are housed, and our general procedures on disposal or reissuance of computer equipment.

Procedures for "Physical Security of PHI and e-PHI

**Facility Access Controls**

Access to areas of our facility that contain our information system components will be granted only to those with a verifiable and approved business need to have access.

All District staff members will be issued identification cards or badges for security purposes. These badges and identification must be displayed at all times while on the premises.

Access control will be established with physical hardware that prevents improper or inadvertent entry into a secure area. This hardware may include combination locks, swipe cards, smart cards and other devices on all doors housing our information system equipment.

The District will retain facility security of any areas used within a building owned or under the control of another entity. In other words, any space in a building that is shared with another entity will be maintained at the same level of security as if the District owned the space. Specifically, we will protect that area from access by others in the building who are not part of the District.

Disabling or circumventing any of the physical security protections is strictly prohibited. Any problems with physical security measures must be reported to your supervisor or the Information Security Officer.

Contingency Operations. The District has established procedures that allow facility access in support of restoring lost data under our disaster recovery plan and emergency mode operations plan in the event of an emergency that could compromise our electronic information system.

Facility Security Plan. The Information Security Officer will be responsible for developing a facility security plan that protects our buildings from unauthorized physical access, tampering, and theft.

The plan will incorporate hardware to limit access to our buildings to only those persons with proper keys and/or access codes.

The Information Security Officer will maintain a current list of all staff members who have authorization to access our facilities.

Access Control and Validation Procedures. Access to various areas of the facilities will be based on the role of the staff person and their need to access a particular area.

Access to locations that house information system infrastructure will have the greatest limitations on access, and access to these critical areas will be reviewed frequently by management and the Privacy/Information Security Officer.

All security devices, including locks, key pads, and other access devices will be well maintained.

**Workstation Security and Use**

A "workstation" is defined as any electronic computing device, such as a desktop computer, laptop computer, PDA, or any other device that performs similar functions, and electronic media stored in its immediate environment.

All workstations will be evaluated to consider the procedures that must be followed to ensure the security of patient and other critical information. The environment will be considered (such as if the workstation is in a large room with cubicles and no fixed walls, the back of an ambulance, a crew room or report writing room, etc.)

General principles of our workstation security program include the following:

- All workstations (including both fixed locations such as in our billing or business office, as well as mobile stations such as with portable workstations equipped for field use) are set with password protection so that the computer may not be accessed without the proper password.
- All workstations are set up to go "inactive" after a set time period so that if the staff member leaves the workstation and forgets to logout and shut down, access will not be permitted without the proper password.
- Procedures are established for each work area, depending on the nature of the work area to limit viewing of workstation device screens to only those operating the workstation wherever possible.
    - For example, in office areas, all screens will be pointed away from hallways and open areas. The screens will be pointed away from chairs or other locations in the office where unauthorized persons, such as patients, may sit within that office.
    - In field operations, ambulance personnel will need to follow procedures to ensure that the workstation device is not left in an open area, such as a countertop in the Emergency Department.

- Workstations will be set so that staff members may not inadvertently change or disable security settings, or access areas of the information system they are not authorized to access.
- Only those authorized to access and use the workstation will be permitted to use the workstation.
- No software may be downloaded or installed on the workstation in any manner without prior authorization. (This prohibition includes computer games, screen savers, and anti-virus or anti-spam programs)
- All staff members will lock or logoff the workstation whenever it is left unattended.
- All portable workstation devices will be physically secured wherever possible when not in use. Laptops will be locked with security cables and PDAs and other handheld devices will be locked in their cradles or in an appropriate storage compartment when not in use.
- Use of any dial up modems and remote access software to access the information system off site must be approved by the Privacy/Information Security Officer.
- Multiple network interface cards (NICs) that allow simultaneous network connections shall not be used in individual workstations unless approved by the Privacy/Information Security Officer.

**Device and Media Controls**

The District carefully monitors and regulates the receipt and removal of hardware and electronic media that contain e-PHI, PHI and other patient and business information into and out of our stations and other facilities. These controls pertain to the movement, re-use, or disposal of hardware and media within the District.

As a general rule, simple deletion of files or folders is not sufficient to ensure removal of the file or data. This simply removes the directional "pointers" that allow a user to find the file or folder more readily. Deleted files area usually completely retrievable with special software and computer system expertise.

Disposal of hardware and electronic media should be consistent with the following:

- Sanitizing Hard Disk Drives. All hard disk drives that have been approved by the Privacy/Information Security Officer for removal and disposal (or taken out of active use) shall be sanitized so that all programs and data have been removed from the drive. The District will follow industry best practices (such as the U.S. Department of Defense clearing and sanitizing standard – DoD 5220.22-M) when cleaning off hard drives.
    - Proper sanitizing usually involves a reformatting of the hard drive in a secure manner with an approved wipeout utility program. Degaussing software may need to be used to ensure total removal of files.
    - No hard drive will be reissued or sold outside of the district, but will be destroyed by the District's IT contractor once fully sanitized
- Accountability. The District tracks the movement of all computer hardware, workstations, and data storage devices. Movement both within the organization and outside the organization is tracked. A logbook is maintained to record the movement of all hardware and electronic media that is sanitized, reissued, or backed up and stored. The Information Security Officer oversees this accountability log.

- Data Backup and Storage. Each information system area will create an exact copy of all e-PHI when necessary immediately prior to any movement or disposal. This procedure is in addition to the standard routine backup protocol to ensure that all e-PHI is preserved before potential compromise.

**A.23.19 Electronic Information System Activity Review and Auditing**

The District is responsible for ensuring the privacy and security of all patient information that we create, receive, or use under both the Privacy Regulations (Privacy Rule) and the Security Regulations (Security Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

One aspect of the District's compliance program is to ensure that activity that takes place on our electronic information system can be "tracked" and documented so that quality assurance procedures will detect and address problems with the system. In other words, we need to be able to "look back" at our system and be able to identify the specific actions that have taken place such as timing and completion of back-up procedures, tracking server file access, and tracking power interruptions and other unusual events that could compromise our system and threaten the integrity of PHI and e-PHI.

Procedures for "Device and Media Controls"

To ensure adequate device and media controls:

- The Information Security Officer will develop procedures to document use of PHI and e-PHI within the information system to track usage.
- The Information Security Officer will review the records of information system activities, including a review of audit logs, security incident tracking reports, back-up records, etc.
- Records of use will include, at a minimum:
  - The date of the use
  - A brief description of the PHI or e-PHI that was used
  - A brief statement as to what the PHI or e-PHI was used for and the disposition of that use
- Uses need not be documented for purposes of an audit trail if the use is made entirely within the internal information system and the use did not involve any outside parties.
- The manner in which the disclosures that are required to be logged under the Privacy Rule were made (PHI that is not related to treatment, payment or health care operations) shall be recorded and tracked. (Example: If the disclosure was made to a nursing facility by electronic mail, that fact should be documented as to when the transmission was made, the specific content of the transmission, who was responsible for requesting it, and who made the transmission.)

**A.23.20 Staff Member Medical Records**

This policy is to ensure the proper protection of that information so that no staff member inappropriately accesses another staff member's medical information, unless permitted by law or regulation. This policy applies equally to management and non-management staff members.

Procedures for “Staff Member Medical Records”

The District will, to the extent required by law, protect medical records it receives about employees or other staff in a confidential manner. Generally, only those with a need to know the information will have access to it and, even then, they will only have access to as much information as is minimally necessary for the legitimate use of the medical records.

All staff member medical information will be kept in a locked office or a locked file cabinet. Any staff member medical information in electronic form will only be accessed by management personnel authorized and permitted under the law to access that information.

In accordance with laws concerning disability discrimination, all medical records of staff will be kept in separate files apart from the employee’s general employment file. These records will be secured with limited access by management.

In accordance with the Privacy Rule of the Health Insurance Portability and Accountabilities Act, medical records that are not considered employment records will be treated in accordance with the safeguards of the Privacy Rule with respect to their use and disclosure.

Employment records are not considered to be protected health information, or PHI, subject to HIPAA safeguards, including certain medical records of employees that are related to the job. These employment records not covered under HIPAA include, but are not limited to: information obtained to determine my suitability to perform the job duties (such as physical examination reports), drug and alcohol tests obtained in the course of employment, doctor’s excuses provided in accordance with the attendance policy, work-related injury and occupational exposure reports, and medical and laboratory reports related to such injuries or exposures, especially to the extent necessary to determine workers’ compensation coverage.

Nonetheless, despite the fact that such records are not considered HIPAA protected, the District will limit the use and disclosure of these records to only those with a need to have access to them, such as certain management staff, the District’s designated physician, and state agencies pursuant to state law.

With respect to staff members of San Juan County Public Hospital District No. 1, only health information that is obtained about staff in the course of providing ambulance or other medical Districts directly to them is considered PHI under HIPAA. In other words, if the District provides ambulance service to an employee, the protections typically given to such information to our ambulance District patients applies to the employee. These protections are subject to HIPAA exceptions, such as in the situation in which the staff member used the District involved in a work-related injury while on duty.

As another example, if the District receives a staff member's medical record in the course of providing the employee with treatment and/or transport, it does not matter the District happens to be the employer – that record is PHI. If, however, the employee submits a doctor's statement to a supervisor to document an absence or tardiness from work, the District does not need to treat that statement as PHI.

Other health information that could be treated as employment related, and not PHI, includes medical information that is needed for the District to carry out its obligations under the FMLA, ADA and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, drug screening results, workplace medical surveillance, and fitness-for-duty-tests of employees.

If you have any questions about how medical information about you is used and disclosed by San Juan County Public Hospital District No. 1, please contact our Privacy Officer.

## A.24 MARKETING AND PUBLIC RELATIONS

### A.24.1 General Public Relations Policies

San Juan County Public Hospital District No. 1 is a taxpayer supported junior taxing district and municipal corporation. It is important that the District be accountable to the public. It is therefore an imperative that the District communicate regularly and openly with the public through the press, publications, mailers, social media, Board meetings, and any other venue to connect with the public we serve.

It is important not only that the District report to the public its activities, but that the public be made aware that these services are available to them, what they cost, and how they are accessed.

Additionally, Village at the Harbor also relies on enrollment for its financial sustainability, and marketing is a valuable and important tool to accomplish that objective. The more residents are enrolled consistently in Village at the Harbor, the less tax money must be utilized to support it.

Procedures for "General Public Relations Policies"

Village at the Harbor may specifically utilize a 1 – 3-year marketing plan approved by the Superintendent.

The Public Information Officer will be responsible for managing the following, under the direction of the Superintendent:

- Mailers – the District will send out quarterly mailers
- Social Media posting should occur regularly
- Websites should be updated regularly and be up to date
- Paid advertising may be used at the discretion of the Superintendent, such as for hiring, legal notices, etc.

### A.24.2 Media

All media inquiries should be referred to Superintendent or a designed Public Information Officer. The Superintendent or the Superintendent's designee must approve all press releases, publications, speeches or other declarations made on behalf of the District. This does not include Elected Officials who may issues press releases etc. on behalf of their specific Elected Office but may not speak on behalf of the District unless specifically authorized.

Procedures for "Media"

The Superintendent or Agency Head or Elected Official may authorize specific employees to respond to media inquiries, either in a particular situation or on an ongoing basis. The Superintendent may issue Standing Orders authorizing Agency Heads to speak on certain topics or in certain situations.

Unless an employee has received direct authorization to communicate with the media on behalf of the District, the employee shall not respond to media inquiries and shall instead refer the inquiry as instructed above.

District employee interactions with the public or other third parties should be courteous and professional at all times. This expectation applies even in those situations where a member of the public is being discourteous. To determine how to proceed in dealing with a particular individual, employees should seek the assistance or intervention of a supervisor.

## A.25 TESTIFYING IN COURT

### A.25.1 Requests to Testify in Court

District employees do not testify upon request in court about business concerns, patients, or any aspect their job for San Juan County Public Hospital District No. 1. All testimony requests received should be immediately directed to their supervisor, who will respond on behalf of the District.

### A.25.2 Subpoena to Testify in Court and Litigation

The District's employees will not testify in court unless compelled to do so by the court or if the District is directly involved in the litigation in question.

District employees should only testify following consultation with management and the District's attorneys as applicable.

# Administrative Policies and Procedures

## Appendices

## Appendix A: Organizational Chart and Staffing Levels

*No organizational chart available at this time.*