

RECORD RETENTION POLICY FOR SAN JUAN COUNTY PUBLIC HOSPITAL DISTRICT #1

PURPOSE

The purpose of this Policy is to establish guidelines for record retention. This Policy applies to all San Juan County Public Hospital District #1 employees and officials.

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.

POLICY

All Public Records are required to be retained according to the Retention Schedule, 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):
 - o Correspondence or memorandum related to the official business of the District.
 - o Original reports.
 - o Policy and procedure directives.
 - o Agenda and meeting minutes.
 - o Documents related to legal or audit issues.
 - o Messages documenting District actions, decisions, operations and responsibilities.
 - o Documents related to District transactions.
 - o Appointment calendars.

- Records that are not likely Public Records and therefore have no retention value:
 - o Information-only copies of documents that do not relate directly to the functional responsibility of the District or the department that receives them.
 - o Personal messages or announcements not related to the official business of the District (i.e. cake for someone's birthday in the break room).
 - o Phone message slips that do not contain information related to the official business of the District.

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.

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 departments 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.

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.

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.

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.

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.

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.

DESTRUCTION OF PUBLIC RECORDS

The District has retained the services of Shred-IT 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.