



Records Management Guidance

Privacy Considerations

Records containing personal information should be protected and handled with care in accordance with applicable laws and best practices. In addition to personal information, you may also handle records containing confidential information, such as attorney client privilege records. This document provides guidance and best practices on how to manage County records that contain personal or confidential information.

Definitions

Term	Working Definition	Examples
Personally Identifiable Information (PII)	Information that can be used to identify an individual Definition NIST SP 800-122 , RCW 42.56.590(10)	Name in addition to address, social security number, date and place of birth, mother’s maiden name, biometric records, etc.
Protected Health Information (PHI)	Individually identifiable health information, which includes PII, with the addition of medical diagnosis, treatment or payment information Definition 45 C.F.R. §160.103 , RCW 70.02.010(17)	Test results, x-rays, scans, physician’s notes, eligibility approvals, claims, and remittances.
Attorney Client Privilege	Legal concept that protects communication between attorneys and their clients for the purpose of seeking or providing legal advice. Attorney Client Privilege does not expire.	Emails, letters, text messages made in confidence that relate to legal advice. May or may not be related to litigation.
Attorney Work Product Privilege	Legal concept that protects attorneys’ mental impressions, thoughts, and legal analysis, related to existing or anticipated litigation. It also protects information gathered by a client, for existing litigation or in anticipation of litigation, at an attorney’s direction.	Emails, letters, text messages that reflect an attorney’s mental impressions related to existing or anticipated litigation.



King County Records Management Program
206-477-6889 – records.management@kingcounty.gov
www.kingcounty.gov/recordsmanagement



Records Management Guidance

Privacy Considerations

Best Practices for Record Creation

- Be mindful about how you document your work. Collect only the minimum amount of personal information needed to accomplish a specific purpose.
- Restrict access to records with personal or confidential information to only those who need it to accomplish a specific purpose.
- Before receiving records with personal information in them, be transparent with those who are providing the personal information as to why the information is needed and if possible, allow them to opt out of providing personal information.

Best Practices for Record Storage and Retention

- Store active records in a location where access can be restricted to only staff who need access to view them.
- Refer to your agency's [retention schedule](#) to ensure records are retained and disposed of according to the law. Records deemed [transitory](#) should be destroyed as soon as they are no longer needed.
- Content Manager is the official repository for County records. Using Content Manager to store sensitive information, including but not limited to PII (Personally Identifiable Information) and PHI (Protected health information), provides the highest security standards for government agencies in the United States. For more information, review [Content Manager Security and Access](#).

Best Practices for Destruction of Records Containing Personal or Confidential Information

If your records are stored in Content Manager or the Records Center, the disposition process is initiated automatically on an annual basis once records have met their retention requirements, except that records must be retained longer if there is a public records request or legal hold for the records. Physical records containing PII or PHI are securely shredded by an outside vendor. Electronic records are deleted from Content Manager.

When dispositioning records containing personal or confidential information within your agency, you must submit a [disposition request](#) form in Content Manager. Once the form is approved then electronic records should be deleted, ensuring that duplicates and trash are also deleted.

At the appropriate time, paper records and physical media (e.g. CD, thumb drives, x-rays, hard drives, etc.) containing personal or confidential information should be destroyed using a secure method. The King County Records Center contracts with an outside vendor to offer this service. To make the request, check the “yes” box on the [disposition request](#) to indicate you want the Records Center to pick up and destroy your physical records and media. Physical media should be packaged separate from paper records.

Reminder

Certain records might also be exempt from *public* disclosure under the Public Records Act. For information about records that might be exempt from public disclosure, reach out to your Public Records Officer.



King County Records Management Program
206-477-6889 – records.management@kingcounty.gov
www.kingcounty.gov/recordsmanagement