Attachment F
Data Destruction Information and References

State of Alaska
Department of Health & Social Services

This is an overview of the State of Alaska and Federal Sources data destruction requirements for confidential information as applicable to the State of Alaska, Department of Health & Social Services. The department recognizes confidential information, information that identifies or could identify an individual, as personally identifiable information (PII) as defined in OMB Memorandum M-07-1616.

> PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual. (GSA.gov)

A DHSS applicable example of this would be a data set that includes an individual's name and one other identifier such as, a social security number, date of birth, driver's license number, account number, password, employee id, or other access codes.

There are many laws and regulations defining PII. Here are just a few examples:

- Alaska Personal Information Protection Act (APIPA) (State of Alaska)
- Electronic Protected Health Information (ePHI)
- Personally Identifiable Information (PII)
- Criminal Justice Information (CJI)
- Criminal History Record Information (CHRI)

To meet the department's required standards for destruction of Electronic Protected Health Information (ePHI), Personally Identifiable Information (PII), Criminal Justice Information (CJI), or Criminal History Record Information (CHRI) staff must comply with the most current NIST guidance (currently NIST Special Publication 800-88 Revision 1). (Kissel, Regenscheid and Scholl) As outlined in NIST Special Publication 800-88 Revision 1, Appendix A—Minimum Sanitization Recommendations, DHSS requires that staff comply with the appropriate Clear, Purge, or Destroy mechanisms for all media.

Additionally, Alaska Statute 45.48 (State of Alaska) Section 45.48.500 -.590 addresses the Disposal of Records by stating:

> When disposing of records that contain personal information, a business and a governmental agency shall take all reasonable measures necessary to protect against unauthorized access to or use of the records.
>
> Notwithstanding (a) of this section, if a business or governmental agency has otherwise complied with the provisions of AS 45.48.500 — 45.48.590 in the selection of a third party engaged in the business of record destruction, the business or governmental agency is not liable for the disposal of records under AS 45.48.500 — 45.48.590 after the business or governmental agency has relinquished control of the records to the third party for the destruction of the records.
>
> A business or governmental agency is not liable for the disposal of records under AS 45.48.500 — 45.48.590 after the business or governmental agency has relinquished control of the records to the individual to whom the records pertain.

In the HIPAA Disposal FAQ (HHS.gov) the Department of Health and Human Services reiterates that PHI must be sanitized using specific means; see:

> For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

Additionally, the HIPAA Security Series – Topic 3, Security Standards: Physical Safeguards (HHS.gov), outlines the following criteria for device reuse:

> Are policies and procedures developed and implemented that address disposal of EPHI, and/or the hardware or electronic media on which it is stored?
>
> Do the policies and procedures specify the process for making EPHI, and/or the hardware or electronic media, unusable and inaccessible?

References

GSA.gov. *https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act*. 12 01 2020. Web. 19 02 2020.

HHS.gov. *https://www.hhs.gov/hipaa/for-professionals/faq/575/what-does-hipaa-require-of-covered-entities-when-they-dispose-information/index.html*. 18 02 2009. Web. 19 02 2020.

—. *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf*. 03 2007. Web. 19 02 2020.

Kissel, Richard, et al. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf*. 12 2014. Web. 19 02 2020.

State of Alaska. *http://www.akleg.gov/basis/statutes.asp#45.48*. 2019. Web. 19 02 2020.