



# **Electronic Signatures**

Ashley Cockerham  
Medical Radiation Safety Team

## Summary of Issue

- More and more documents are developed and stored electronically
- NRC permits the use of electronic media to **produce** and **store** records that are inspected at the licensee's facilities

## **Summary of Issue (cont)**

- 10 CFR Part 35 is silent on the topic of electronic signatures
- Documents that require signatures by specific individuals can be signed electronically

## Summary of Issue (cont)

- Records licensees keep vs documents submitted to NRC
- Electronic signature vs digital signature
  - <http://www.nrc.gov/site-help/e-submittals/faqs.html>

# Medical Licensee Record Requirements

- 35.40(a), 35.40 (c)
- 35.80(a)(1)
- 35.2040
- 35.2080
- 35.2024(a); 35.2024(b)
- 35.2026
- 35.2632(b)(5)
- 35.2642(b)(9)
- 35.2643(b)(5)
- 35.2645(b)(9)
- 35.2647(a)(5)
- 35.2652(b)(4)
- 35.2655(b)(5)

# NRC Considerations

- How do written signatures function?
  - Unique identification
  - Authentication
  - Non-repudiation

## **NRC Considerations (cont)**

- Other considerations for electronic signatures
  - Data integrity assurance
  - Individual signing must know he/she is signing
  - Concise process: same individual that initiates, concludes
  - Inspection

## **NRC Questions**

- What standards for electronic signatures in medical records are in use or under development?
- How do these standards address the principles of authentication, non-repudiation, data integrity, and access for inspection?
- Do these standards consider any additional key principles?



## **NRC Questions (cont)**

For software applications currently in use

- How does the licensee assure that the signature process is uniquely tied to the individual whose signature is required?
- What provisions does the licensee use to inform persons electronically signing documents that they are entering their signature?

## **NRC Questions (cont)**

- How does the licensee assure that the document being electronically signed cannot be changed after it is signed?
- How does the licensee assure that subsequent changes to the document require a new electronic signature and cannot overwrite the previous versions?

## **NRC Questions (cont)**

- How does the license assure that the electronic signature process affixes the date and time to each electronic signature?
- How does the licensee assure that electronically signed documents and all revisions to the documents are accessible for inspection?

## **NRC Questions (cont)**

- How does the licensee assure that electronically signed documents and all revisions to the documents are retained for 3 years?
- Are any improvements needed for current commercially-available software applications to adequately meet existing standards and principles?

# Summary of Comments Received

5 submissions from public

- Coordinate with other regulatory agencies and accreditation organizations for consistency and compatibility
- Concerns about unnecessary burdens on healthcare providers

## Summary of Comments (cont)

- Accept electronic signatures if the issues raised by NRC are addressed and state laws do not prohibit actions.
- Recommend that NRC poll each state to determine if laws would prohibit any of the actions.

## Summary of Comments (cont)

- Portable Document File (PDF)
  - 10+ years
  - Digital signing
  - Prevent revisions
  - Secure
  - Globally accepted

## Summary of Comments (cont)

- VA electronic health record system
  - Proprietary electronic health record system in nuclear medicine and other applications
  - Does not adhere to any specific standard
  - Cannot be validated outside of VA's electronic health record
  - VA moving away from system



## Summary of Comments (cont)

- NIST FIPS 201
  - PIV cards
  - Digitally sign documents using PKI
  - Addresses authentication, non-repudiation, data integrity, and access for inspection

## **Request to ACMUI**

- NRC is seeking information or a “benchmark” on current practices for the use of electronic signatures for medical records.
- NRC is seeking recommendations from the ACMUI on acceptable criteria for using electronic signatures.

# Acronyms

- CFR – Code of Federal Regulations
- FIPS – Federal Information Processing Standards
- FR – *Federal Register*
- NIST – National Institute of Standards and Technology
- PIV - Personal Identity Verification
- PKI – Public Key Infrastructure
- VA – Department of Veterans Affairs

# Questions?