SSH Society for Simulation in Healthcare CERTIFICATION	CREATION DATE February 15, 2012	DATE REVISED July 26, 2024
	POLICY AREA / CATEGORY	DATE APPROVED /EFFECTIVE DATE March 01, 2012
POLICY TITLE RECORDS MANAGEMENT	VERSION	DATE REVIEWED July 26, 2024

SUMMARY & PURPOSE:
This document serves to describe the concepts and principles pertinent to the appropriate management of all certification records (e.g., applicant files) and other documents as appropriate.

DEFINITIONS:
None

POLICY:
It is the policy of SSH Certification to ensure that all records of applicants, candidates, and certificants are managed and maintained in a way that ensures consistency, security, and integrity. Key features of this management of documents includes:

- Only designated SSH staff shall have access to records as needed, the Director of Certification shall be solely responsible for who has access to certification records and data.
    - SSH staff assigned with a certification title (e.g., Certification Coordinator) shall have access.
    - Other SSH staff shall be granted access as appropriate to perform job functions to support certification
- Vendors may be granted access to files and/or data as appropriate to perform job functions. This is determined by the Director of Certification.
- Volunteers (e.g., Subject Matter Experts) shall never be given direct access to applicant, candidate, or certificant records. Certification Council Chair or Vice Chair may be given limited access to candidate records at the discretion of the Director of Certification
- Volunteers will be provided access to documents needed to perform their work as provided by SSH Certification staff and appropriate to the task (e.g., Dropbox, SimConnect)
- Any records that are kept with any vendor (e.g., testing vendor) are the sole property of SSH and shall be returned to SSH on conclusion of any contractual agreements.
- Applicant, candidate, and certificant records shall be kept as follows:
    - For 10 years or the life of the contract with the vendor.
    - If a vendor change is initiated by either party, then SSH staff shall work with vendor to transfer data that must be maintained regarding examinations.
- Names, locations, and certification of currently certified individuals shall be made publicly available on the certification website and updated at appropriate intervals.
- Requests for verification of certification status can be made by email through the website.
- SSH staff shall adhere to all applicable U.S. laws and/or agreements for retention, disposal, and destruction of any documents (real or virtual).
- Applicant, candidate, and certificant identifying information shall be removed to preserve the integrity of any review process (e.g., complaints or appeals) where individuals may have access to that particular individual’s record.
- Written permission shall be obtained prior to releasing any applicant, candidate, or certificant information.
- Only applicants, candidates, or certificants can request any action on their behalf (e.g., payments, changes in records, release of information).

SCOPE/APPLICABILITY:
This applies to all applicant, candidate, and certificant records including hard copies, and electronic copies no matter where they are stored (on a computer, in the cloud, etc.).

PROCEDURES TO ENSURE COMPLIANCE:

- SSH staff shall be responsible for ensuring the appropriate management of all documents.

- Any potential violation of records shall be reported to the Director of Certification for investigation.

SUPPORTING/REFERENCE DOCUMENTATION:

- None

RELATED POLICIES & PROCEDURES AND ASSOCIATED FORMS:

- Confidentiality Policy
- Prometric Exam Security Policy

ASSOCIATED NCCA STANDARD(S):

- 9, 9A, 9B, 9C, 9D, 10B, 10C, 10E

POSTED PUBLICLY: YES