SIU School of Medicine
Identity Protection Policy
Frequently Asked Questions

The purpose of the following Frequently Asked Questions is to provide general guidance to employees of the School of Medicine (SOM) who either Request, Receive, Use, Retain, Disclose, or Destroy a document containing an individual's Social Security Number (SSN) in performance of their assigned SOM responsibilities.

Q. Who has access to a Social Security Number (SSN) at the SOM?

A. Access to SSNs will be limited to only those SOM employees who have a University business need for the information.

Q. As an employee of the SOM, what must I disclose or tell an individual when requesting their SSN?

A. You must inform the individual whose SSN is being requested as to the purpose(s) and use(s) in obtaining the SSN. A paper-based statement, electronic statement/notification, or a written statement added to an existing business form which the individual receives, are acceptable methods of disclosure. Departments/units may use the standard Statement of Purpose (SOP) or may modify this statement to meet their specific needs.

Q. As an employee of the SOM, can I request that an individual transmit their SSN over the internet or may I transmit their SSN over the internet?

A. Employees shall not request nor require an individual to transmit their SSN over the internet nor should an employee transmit a SSN over the internet, or through an email service, unless the SSN is encrypted. E-mail accounts with standard password accesses are not considered secure connections.

Q. May I receive/request a SSN from anyone other than the individual to whom it is assigned?

A. Receiving a SSN from anyone other than the individual whose SSN is assigned is only appropriate if the disclosure is part of the SOM's business processes, and the SSN owner has received a disclosure as to how their SSN will be utilized including any secondary uses/disclosures. Internal sharing of SSNs is permissible, so long as the SSN owner has been provided with the appropriate disclosure as to how their SSN will be utilized, and the appropriate data security measures have been taken.

Q. As an employee may I disclose a SSN to a SOM contractor or subcontractor?

A. If for any reason the SOM must disclose a SSN to a contractor or subcontractor, the SOM must request and receive a copy of the contractor's or subcontractor's policy on how they will protect the SSN/data in their operations or processes. Additionally, the SSN owner must have been advised as to how their SSN will be utilized including any secondary uses/disclosures.

Q. What must I do if a document is requested, that displays an individual's SSN, and is requested by an outside agency?

A. Unless otherwise authorized by law, an individual's SSN will be redacted (blackened out) before releasing the document for public inspection or copying the document. Using SSNs requested from an individual shall be accomplished in a manner that makes the Social Security Number (SSN) easily redacted if required to be released as part of a public records request.

Q. How do I protect/store documents that contain an individual's SSN?

A. The SOM will ensure to the extent practicable, the confidentiality of SSNs that it possesses. SSNs are considered sensitive data elements and will be managed, protected, and secured in locked file cabinets with restricted access to only those employees who need the SSN in conducting the affairs of the SOM.

Q. How long should I maintain and store records which contain a person's SSN?

A. As soon as allowable under state, federal or University policy, a document in either electronic or paper format containing a SSN where the need for the information is no longer relevant, should be securely destroyed as per University policy. All questions pertaining to the SOM's Records Management Program and record retention/destruction schedules should be directed to Records Management unit at 217.545-1282 SOM mail code 9668.

Q. Who is the point of contact should I have additional questions regarding the SOM's Identity Protection Policy?

A. You should contact the Chief Compliance Officer at (217) 545-8532 or clong@siumed.edu.