SOUTHERN ILLINOIS HEALTHCARE

System **Policy and Procedure**

Title:	Biometric Information Use and Collection	**Number:**	SY-LE-010
Applies to:	Legal, IT, Human Resources	**First Created:**	1/28/19
Issuing Dept:	Legal	**Last Revised:**	
Approved by:	William F. Sherwood, VP/General Counsel		

I. POLICY

Southern Illinois Hospital Services (SIHS) complies with the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 *et seq*. Biometric information is unlike other unique identifiers used to access sensitive information. Biometrics are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at a heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions. As the use of biometrics is growing in healthcare, SIHS is well served to regulate the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

II. DEFINITIONS

Biometric Identifier – a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, parts, blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants. Biometric identifiers do not include biological materials regulated under the Illinois Genetic Information Privacy Act. Biometric Identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric Identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

Biometric Information – any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

Written Release – informed written consent or, in the context of employment, a release executed by an employee as a condition of employment

III. RESPONSIBILITIES

1.0 Human Resources maintains and safeguards records applicable to the Illinois Biometric Information Privacy Act as identified in this policy.

2.0 IT maintains and safeguards the information technology involved in the storage, collection, and maintenance of the Biometric Information and Biometric Identifiers, except those items which are contractually obligated to be performed by a third party.

3.0 General Counsel's office

3.1. Approves written release

3.2. Reviews and approves any associated contracts

IV. EQUIPMENT/MATERIALS

1.0 Release/consent form

2.0 Contracts

V. PROCEDURE

1.0 Biometric Identifiers and Biometric Information are maintained in accordance with the Illinois Biometric Information Privacy Act.

2.0 Biometric Identifiers and Biometric Information may be collected after the individual, whose information is being collected, has signed a written release.

2.1 The written release to be signed is approved by the General Counsel's office prior to signature.

3.0 Biometric Identifiers and Biometric Information may be stored for three (3) years after the individual's last interaction with SIHS or when the initial purpose for collecting or obtaining such identifier or information has been satisfied, whichever one comes first.

4.0 At no time shall SIHS contract with or enter into an agreement with an outside party or vendor to sell, lease, trade, or otherwise profit from a person's biometric identifier or biometric information.

5.0 SIHS will not disclose, redisclose, or otherwise disseminate a person's biometric identifier or biometric information unless:

5.1 The subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure

5.2 The disclosure or redisclosure is required by State or federal law or municipal ordinance or

5.3 The disclosure is pursuant to a valid warrant or subpoena issued by a Court

6.0 If Biometric Identifiers or Biometric Information is to be collected, the following process is followed:

6.1 The individual providing the information is provided an approved consent form for the particular device, software, or vendor which will be storing the information.

6.2 The individual then signs the consent form.

A. A copy of the signed consent form may be provided to the individual upon request.

6.3 The individual may then provide the sample including the Biometric Identifiers or Biometric Information.

6.4 For employees of SIH, the signed consent form is then delivered to Human Resources for storage pursuant to section 1.0 of Responsibilities under this policy.

7.0 Prior to entering a contract where Biometric Identifiers or Biometric Information is used or collected by SIHS or another party, the contract is reviewed and approved by the General Counsel.

VI. DOCUMENTATION

1.0 HR maintains identified records.

2.0 General Counsel maintains copies of approved contracts.

VII. CHARGES

N/A

Additional Approvals and Review/Revision Dates			
Review Dates:			
Revision Dates:			
Replaces:	N/A		
Additional Approvals:	**Name (print)** Gerald Mourey Pam Henderson	**Title** VP/CIO VP/Human Resources	**Signature**