TOPIC:	Biometric Information Security Policy	POLICY NO.:	
SECTION:		DATE CREATED:	7/26/16
DATE REVIEWED:		DATE REVISED:	
		PAGE:	1 of 2

PURPOSE

To define the policy and procedures for collection, use, safeguarding, storage, retention, and destruction of biometric data collected by Symbria.

DEFINITIONS

- Biometric data means personal information stored by Symbria about an individual's physical characteristics that can be used to identify that person. Biometric data can include fingerprints, voiceprints, facial shape, or scan of hand or face geometry.

POLICY

- Symbria's policy is to protect and store biometric data in accordance with applicable standards and laws including, but not limited to, the Illinois Biometric Information Privacy Act.
- An individual's biometric data will not be collected or otherwise obtained by Symbria without prior written consent of the individual. Symbria will inform the individual of the reason his or her biometric information is being collected and the length of time the data will be stored. A sample consent statement is included in this policy and will be tailored to fit the type of biometric data collected.
- Symbria will not sell, lease, trade, or otherwise profit from an individual's biometric data.
- Biometric data will not be disclosed by Symbria unless (a) consent is obtained, (b) disclosure is necessary to complete a financial transaction requested or authorized by the subject, (c) disclosure is required by law, or (d) disclosure is required by subpoena.
- Biometric data will be stored using a reasonable standard of care for Symbria's industry and in a manner that is the same or exceeds the standards used to protect other confidential information held by Symbria.
- Symbria will destroy biometric data when the initial purpose for obtaining or collecting such data has been fulfilled.
- Symbria reserves the right to amend this Biometric Information Security Policy at any time.
- A copy of this policy will be made publically available at www.symbria.com.

PROCEDURE

1. Symbria collects, stores, and uses employee fingerprint data for the purpose of giving employees secure access to Symbria's corporate office and pharmacy locations. Fingerprint data may also be collected and used to provide access to drug cabinets or other pharmacy-related equipment or machines.
2. Prior to collecting an employee's fingerprint data, Symbria will obtain the consent of the employee.

3. Symbria will store, transmit, and protect biometric data using the same standard of care and security controls it provides the protected health information in its possession.
4. Symbria's information technology department will permanently destroy an employee's biometric information from Symbria's systems upon the employee's termination from Symbria.
5. In the even Symbria begins collecting biometric data for any additional purpose, Symbria will update this procedure.

SAMPLE CONSENT TO COLLECTION OF BIOMETRIC DATA

Your fingerprint will be collected and stored by Symbria for the purpose of verifying your identity for access to the corporate office or pharmacy. Additionally, if you work at the pharmacy, your fingerprint may also be collected and used to provide you access to drug cabinets or other pharmacy-related equipment or machines. Your fingerprint data will not be disclosed by Symbria without your consent unless the disclosure is required by law or by subpoena. Your fingerprint data will be permanently deleted from Symbria's systems when you leave the company. A copy of Symbria's Biometric Information Security Policy is available upon request and is posted at www.symbria.com. By signing below, you consent to Symbria's collection, use, and storage of your fingerprint for the above defined purpose.