

Information Security Standard

Biometric Identifiers

- All BJC HealthCare Hospitals and Healthcare Service Organizations (HSOs) operating in Illinois align with the *Illinois Biometric Information Privacy Act* for the collection, use, safeguarding, storage, retention, and destruction of *Biometric Information*.
- *Biometric Information* means any information, regardless of how it is captured, converted, stored or shared, that is based on an individual's "*Biometric Identifier*," as that term is defined below.
- *Biometric identifiers* include a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.
- Biometric identifiers do not include demographic data, photographs, written signatures, physical descriptions such as height, weight, hair color or eye color, writing samples, human biological samples used for valid scientific testing or screening, tattoo descriptions or other items or types of information specifically excluded from the definition of Biometric Identifiers under the Illinois Biometric Information Privacy Act.
- BJC's standard is to protect and store Biometric Information in accordance with applicable standards and law including, but not limited to, the *Illinois Biometric Information Privacy Act*.
- An individual's *Biometric Information* will not be collected or otherwise obtained by a BJC HSO operating in Illinois without prior written consent of the individual or his/her legally authorized representative. Such HSO will inform the individual of the reason his or her Biometric Information is being collected and the length of time the information will be stored.
- HSOs will not sell, lease, trade, or otherwise profit from an individual's Biometric Information.
- HSOs will not disclose Biometric Information 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 Information will be stored using a reasonable standard of care for the health care industry and in a manner that is the same as or exceeds the standards used to protect other confidential information held by the HSO.
- HSOs will destroy Biometric Information when the initial purpose for obtaining or collecting such information has been fulfilled or no later than within three (3) years of the individual's last interaction with the HSO.
- BJC reserves the right to amend this policy at any time. A copy of this policy will be made publicly available in the department(s) using equipment collecting biometric information.