ST. BERNARD HOSPITAL

326 West 64th Street, Chicago, IL 60621

BIOMETRIC TECHNOLOGY (BIPPA) POLICY

POLICY ON BIOMETRIC TECHNOLOGY

St. Bernard Hospital contracts with a vendor to provide finger printing services in connection with the background checks conducted during the hire process and as may be required by the IL Healthcare Worker Background Check Act and implementing regulations. The Company's vendor collects and maintains fingerprint images (electronic) or finger print cards (hard copy) for purposes of completing the Company's criminal background check process. This policy sets forth the storage, retention and destruction information for an individual's finger print images collected as part of this process. This policy is intended to advise employees of the nature and extent any system in use by St. Bernard (the "Company") which may be considered biometric information or biometric identifiers subject to the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, et seq.

Disclosure

1. The finger print image, card scans or data derived from the scan may be collected by, used and stored by the Company's vendor. Currently, the vendor is Accurate Biometrics, Inc. The Company does not collect, store, retain or otherwise obtain the fingerprint images (electronic or hard copy) collected by the vendor. The finger print images may be disclosed or disseminated to various law enforcement agencies or background check vendors for purposes of completing the criminal background check.

2. The Company will not sell, lease, trade, or otherwise profit from the stored image (electronic or hard copy) of the employee's fingerprint image, scan or data derived from the image; however, the Company may pay a vendor providing the technology for products or services utilized by the Company.

Retention and Destruction Guidelines

The Company does not store or transmit fingerprint image scans, card scans or data derived from the scan and therefore, it does not retain any information requiring destruction. Pursuant to the vendor's policy, the fingerprint image scan, card scans and/or data derived from the scan will be stored by the vendor for up to sixty days from the date of receipt, fingerprint capture or card scan date or the date last modified in the case where the original fingerprint or card scan date was modified.

Storage, Transmission and Protection

The Company does not store or transmit fingerprint image scans, card scans or data derived from the scan. Pursuant to the vendor's policy, all identifiers and other biometric information which are stored electronically are encrypted both in transit and at rest from the time of capture and while stored on a local server or backup hard drive. If they are backed up offsite, they are securely encrypted in the cloud so the cloud server provides no third-party access to them. Secure electronic "delete" functions take place after which the identifiers and other biometric information are no longer accessible and permanently destroyed on the applicable hard drive, backup drive, or external cloud servers so the identifiers and other biometric information are no longer accessible after the time frames noted in this Policy. Hard copy scans are converted into electronic format and the physical documents are destroyed after 30 days, per the vendor policy.