VALIANT	**LEG-007.02 Biometric Privacy Procedure**	**CORPORATE PROCEDURE**
	Effective: November 3, 2022	**Version:** 2.0
	Function: Legal	**Approved by: /s/** General Counsel

Procedure

This procedure establishes guidelines for Valiant's use of Biometric Information. Valiant, certain of its vendors providing products and services using biometric data (including the licensor of Valiant's time and attendance software) and/or the Defense Counterintelligence and Security Agency ("DCSA") collect, store, and use biometric data solely for employee identification, fraud prevention, government required security clearance and / or pre-employment hiring purposes.

1. Scope

This procedure applies to Valiant Integrated Services LLC and its subsidiaries (collectively, "Valiant), including all associates, consultants, and technical advisors.

2. Definitions

Biometric identifier: means 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 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 information: means 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.

3. Policy

3.1 Authorization

To the extent that the Valiant, its vendors, and/or the DCSA collect, capture, or otherwise obtain biometric data relating to an employee or contractor, Valiant must first:

- Inform the individual in writing that Valiant or the third party entity is collecting, capturing, or otherwise obtaining the individual's biometric data,and what third party entity will receive the biometric data;
- Inform the employee in writing of the specific purpose and length of time for which the employee's biometric data is being collected, stored, and used; and
- Receive a written release signed by the individual (or his or her legally authorized representative) authorizing the Valiant, its vendors, and/or the DCSA to collect, store, and use the individual's biometric data for the specific purposes disclosed by the Valiant, and for the Valiant to provide such biometric data to the specified third party entities.

Valiant, its vendors, and/or the DCSA will not sell, lease, trade, or otherwise profit from employees' biometric data; provided, however, that Valiant's vendors may be paid for products or services used by Valiant that utilize such biometric data.

3.2. Disclosure

Valiant will not disclose or disseminate any biometric data to anyone other than its vendors providing products and services

using biometric data and/or the DCSA without first obtaining written employee or contractor consent to such disclosure or dissemination unless:

- The disclosed data completes a financial transaction requested or authorized by the individual;
- Disclosure is required by state or federal law or municipal ordinance; or
- Disclosure is required pursuant to a valid warrant or subpoena issued by a court or administrative body of competent jurisdiction.

3.3 Retention Schedule

Valiant shall retain employee or contractor biometric data only until, and shall request that its vendors permanently destroy such data when, the **first** of the following occurs:

- The initial purpose for collecting or obtaining such biometric data has been satisfied, such as the termination of the employee's employment with Valiant, or the individual moves to a role within Valiant for which the biometric data is not used; or
- Within three years of the individual's last interaction with Valiant.

For the Defense Counterintelligence and Security Agency retention of records in its possession is in accordance with applicable Federal law.

3.4. Data Storage

Valiant shall use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic biometric data collected. Such storage, transmission, and protection from disclosure shall be performedin a manner that is the same as manner in which the Valiant stores, transmits and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an individual's account or property, such as genetic markers, genetic testing information, account numbers, PINs, driver's license numbers and social security numbers.

4. References

LEG-007 Global Data Privacy

740 ILCS 14/1, Biometric Information Privacy Act; 41 A.L.R. 7th Art. 4 (2019), State Statutes Regulating Collection or Disclosure of Consumer Biometric or Genetic Information; Practical Law Practice Note w-014-0305, Biometrics in the Workplace. Accessed 3 Nov 2022.

5. Questions or Concerns

For questions regarding this policy, reach out to legal@onevaliant.com.

6. Revision History

Version	Effective Date	Description	Policy Owner
1.0	5/7/2021	Initial Release	
2.0	11/21/2022	Update to Reflect Addition of Fingerprints	