

## Texas Donor Biometric Data Privacy Policy

The operator of the facility at which you are donating blood (center operated by Grifols Bio Supplies, Inc.) or plasma (center operated by Biomat USA, Inc., which is hereafter called with Grifols Bio Supplies, Inc., the “Company”), uses a donor management system managed and supported by a third-party vendor, Haemonetics Corporation (for Biomat USA, Inc.) or MAK-SYSTEM (for Grifols Bio Supplies, Inc.), to ensure proper verification of donors’ identities during the donation screening process. The system uses certain Biometric Data (defined below) solely for this purpose. The Company established this Policy to ensure such data is, and continues to be, reasonably safeguarded and not retained for longer than is necessary. Further, this Policy is intended to comply with any potentially applicable laws including, but not limited to, Texas Business & Commerce Code Section 503.001 (Capture or Use of Biometric Identifier).

### **Definition of Biometric Data for Purposes of This Policy**

Solely for purposes of this Policy, Biometric Data means the encrypted hash value that is generated when a donor scans a fingertip on a Company computer-assisted self-interview (“CASI”) system kiosk finger scanner. During this process, no fingerprints or images of fingers or fingerprints are collected or retained in any form or transmitted outside of the system. Rather, hash values are generated from the scans by an application on the Company’s network called VeriFinger. The resulting hash values are stored securely in the Company’s databases in the United States to the extent they are stored by the Company, but fingerprint images are not collected, saved, or stored. No hash values are transmitted to any other location or third-party.

The phrase “Biometric Data” as used in this Policy includes, but is not limited to, all potentially applicable legal definitions of “biometric identifiers” and “biometric information,” including, but not limited to, data generated from the scan of a finger or fingerprint. In addition, for purposes of this Policy, data or other information derived from a scan of a donor’s finger or fingerprint during the donation screening process is referred to as “Biometric Data” even though it may not meet the definition of “biometric information” or “biometric identifiers” under any potentially applicable law, such as Texas Business & Commerce Code Section 503.001 (Capture or Use of Biometric Identifier).

### **Collection of Biometric Data**

The Company will obtain a written release/consent from each donor using the system. The form must inform the donor of the data being collected; the purpose of the collection; the use, storage and any transmission of the data; and the period of time the Biometric Data is being collected, stored, and used.

### **Use of Biometric Data**

The Company will use the Biometric Data solely for purposes of administering the Donor History Questionnaire to ensure the proper verification of the donor’s identity and, potentially, other lawful purposes. The finger is scanned twice, once to initiate the questionnaire and then again to finalize the questionnaire. Such additional purposes for obtaining a finger scan may include, but are not limited to, conducting audits and investigations, as necessary.

### **Access to Biometric Data**

In general, Company employees are unable to access donor Biometric Data. However, certain authorized Company personnel that require access to the database where Biometric Data is stored could potentially view the hash values. Moreover, to the extent ever necessary, Company attorneys and/or investigators may from time to time need access to donor Biometric Data to conduct audits or investigations. Further, as described herein, Biometric Data may be made available to Haemonetics Corporation (by Biomat USA, Inc.) or MAK-SYSTEM (by Grifols Bio Supplies, Inc.) as needed to operate and maintain the donor management system, including to provide technical support.

## **Disclosure of Biometric Data**

The Biometric Data of donors is currently securely stored on Company server databases located in the United States that may be accessed by certain Company personnel and certain authorized third-parties, including Haemonetics Corporation (for Biomat USA, Inc. donor data) or MAK-SYSTEM (for Grifols Bio Supplies, Inc. donor data) as described herein, who are granted security access by the Company. However, the Company may in the future disclose such Biometric Data to Company-retained attorneys and/or investigators to the extent it is necessary to conduct audits and investigations. In the event additional parties need access to donor Biometric Data for technical support, administration or other lawful purposes, the Company will make available or disclose Biometric Data only after obtaining: (i) written consent to the disclosure for identification purposes from the individual(s) to whom the Biometric Data relates, and (ii) the written assurances from the third-party that the Biometric Data will be safeguarded in accordance with applicable law and best practices.

## **Retention and Destruction of Biometric Data**

The Company shall adhere to its Privacy Policy, which may be found on the Company's website: [www.grifolsplasma.com](http://www.grifolsplasma.com). Consistent with that Policy, the Company will retain donor Biometric Data only for as long as necessary to satisfy the initial purpose for which the Biometric Data was collected. Except as otherwise required by law, including but not limited to, federal or international regulations, the Company will take the actions necessary to permanently delete a donor's Biometric Data from the Company database where it is stored as soon as practicable when eleven (11) months (if donated at Company whole blood center) and six (6) months (if donated at Company plasma center) have elapsed since the donor last scanned a fingertip on a Company scanner as part of the donation screening process. If the individual donates again after that time, s/he will be required to complete the verification process again in order to donate. To the extent this process ever results in a donor's Biometric Data not being deleted within 1 year of the donor's last interaction with the Company of any kind, the donor's Biometric Data will be permanently deleted as soon as is practicable at that time.

## **Safeguarding Biometric Data**

Consistent with the Company's information security policies, procedures and practices, which are incorporated herein by reference, as applicable, the Company shall take reasonable steps to ensure that donors' Biometric Data, regardless of format, is protected from unauthorized access, acquisition or disclosure. Such safeguards shall include storing the Biometric Data on secure Company databases located in the United States, limiting access to donor Biometric Data, and using the minimum necessary donor Biometric Data for a particular permissible purpose.

## **Amendment, Enforcement and Violations**

The Company reserves the right to amend this Policy at any time for any reason.

Grifols Bio Supplies, Inc. or Biomat USA, Inc. shall be responsible for implementing, interpreting and enforcing this Policy, as applicable, in collaboration with other appropriate Company departments and officers.

Employees who violate this Policy shall be subject to discipline up to and including termination of employment.

Last updated May 2023