LookinBody Web: InBody Cloud Data Management Software

Security Policy (as of March 5, 2021)

The LookinBody Web service (https://usa.lookinbody.com) is a service that allows you, the user, to manage all data measured by InBody devices on the cloud using Microsoft Azure's Web Apps. Please refer to the following table for security policies relating to this service.

Certification	
Operational Security Certification	Cloud services are hosted through Microsoft Azure. Biospace, Inc. dba InBody USA: SOC2 certified; ISO 27001 certification planned completion by 2021. LookinBody, LTD (Korea) a subsidiary of InBody Co. Ltd., entrusted with system development and operation to provide services, plans to obtain ISO 27001 certification by 2021. [1]
Payment Security	PCI DSS compliant Automated monthly and yearly payments are processed securely through Authorize.net (https://support.authorize.net/s/article/Is-Authorize-Net-PCI-DSS-compliant)
Application	
Retention of Personal Information or Confidential Information	Hosted on Microsoft Azure's HIPAA compliant server. The LookinBody Web service is based on Microsoft Azure's Web Apps. Microsoft provides access management and intrusion detection systems.[2]
WAF, IDS, IPS Deployment	Protected by Microsoft Azure's IPS (Intrusion Prevention System) Access limited through authorized IP's and users Access and usage logs are automatically recorded
Authentication Method When Using LookinBody Web	ID and password are used, and the following security measures are taken: 1. Login ID Requirement: 5-20 Alpha-Numeric characters, using lowercase letters and numbers 2. Password Requirement: 8-14 Alpha-Numeric characters, with at least 1 upper-case and lower-case letters and numbers. 3. Password Expiration Policy: Pop-Up notification after 3 months of setting previous password (No access restrictions are placed when password is expired) 4. Password Entry Restrictions: Automated Captcha requirement when password is entered incorrectly more than 5 times (No limit is placed to the number of captcha input). 5. Counter Measures against lost IDs' and Passwords: Temporary password is provided to registered email 6. Additional Login Security: 2 Factor Authentication available using email
Authentication method for Downloading Personal Information	Member List Page: Personal Information Download Feature 1. Confirmation of Login Password required to access feature Administrator Login: Export as Excel through Setup 1. Default Security: Confirmation of Login Password required to access feature 2. Additional Security can be added by creating a Master Password Exported Excel file will have the Mobile number identification field masked for the first 6 digit
Logging	Login records can be verified using the using the Check User Log feature available through the Administrator Login in the Setup menu. Logs will be saved by date and contain ID and IP address details
Data Protection	

Database Encryption	Database is encrypted using TDE. Password is sent using AES 256 standards. SSL applied for server communication with InBody devices.
Data Deletion Method	Deletion of data stored on the LookinBody Web service will be permanently removed from the LookinBody Web Portal, however a de-identified copy of the deleted data may be kept by our system for Quality Control and Research purposes. HIPAA/Covered Entities: For compliance with HIPAA, user data will be retained for a period of 6 years even if the user account managing the data is deleted.
Full Data Deletion	For full data deletion: 1. Data will be deleted from the LookinBody Web service portal 2. Data will be deleted from the InBody unit directly 3. Data saved to a user's app will not be deleted; the user shall be personally required to delete app data. All 3 steps must be completed for full data deletion
Restricting Access to Personal Information Data	Certain members of the LookinBody team who oversee system development and operation have limited access to users' personal information for purposes of incident management, as follows: 1. Onsite CCTV in use for 24-hour workstation monitoring with fingerprint recognition for workplace access control 2. Only authorized developers are granted direct access to the cloud servers 3. IP Address restriction in place 4. Dual authentication required to access cloud server management 5. Permission and new user setup limited to top level administrator only 6. Annual inspections performed 7. Monthly inspections of server status and traces external intrusion performed 8. Restrictions and Block Access policies in place upon employee termination
Operation	
System Development and Operation-Side Personal Computer Management	LookinBody, LTD, which is responsible for system development and operation, manages personal computers as follows, not including the above personal information data restrictions mentioned above: 1. Keep Windows 10 Defender up to date 2. Non-use of external recording media 3. Save work logs on Microsoft Azure storage server
Cloud Service Locations	Microsoft Azure Data center is located in the United States (West US) United States user personal information and measurement data remains within US-based cloud servers.
Companies implementing and Utilizing this service	The service started in May 2014 and as of July 2020 over 2000 facilities have registered for the service globally.

[1] For information on "Personal Informaiton Protection Policy" and "Personal Information We Handle", please refer to the Terms of Use and Privacy Policy our website (https://usa.lookinbody.com)

[2] For more information on Microsoft Azure, please visit the Microsoft home page below:

https://azure.microsoft.com/en-us/overview/