ITAMAR MEDICAL Ltd. SECURITY POLICY

[Last Updated: November 4, 2020]

Itamar Medical Ltd. and its affiliates (collectively, the "**Company**" or "**we**") is committed to provide transparency regarding the security measures and policies which it has implemented in order to secure and protect personal data, personal health information and personal identifying information (together "**Personal Data**"), all as defined under applicable data protection law, including without limitations, including without limitations, the EU General Data Protection Regulation ("**GDPR**") and the soon to be going into effect California Consumer Privacy Act ("**CCPA**") and the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") including the Security Standards for the Protection of Electronic Protected Health Information (all collectively shall be defined herein as the "**Data Protection Regulation**").

This information security policy outlines the Company's security, technical and organizational practices.

As part of our data protection compliance process we have implemented technical, physical and administrative security measures to protect Personal Data, including upholding standards of Cybersecurity and Infrastructure Security Agency, the national institute standards and technology and the GDPR TOM requirements.

Physical Access Control

The Company ensures the protection of the physical access to the data servers which store Personal Data. The Personal Data processed by the Company is stored either within the Company's local server farm, or in the Amazon Web Services servers. Further, the Company secures the physical access to its offices (i.e., alarm systems, code locks) and maintain records of any physical access to the protected Personal Data in order to ensure that solely authorized individuals such as employees and authorized external parties (maintenance staff, visitor, etc.) can access the Company's offices. The Company uses a monitoring surveillance measures (i.e. video surveillance) to ensure that unauthorized person shall not enter the Company's offices.

Security Risk Analysis and Management.

The Company conducting an accurate and thorough assessment of the potential risks and vulnerabilities of the Company's Personal Data to ensure the confidentiality, integrity, and availability of electronic protected health information. The Company applies a periodic testing of the Company's disaster plan in order to ensure that the Company can cope with a consummation of any disaster and emergency case. The Company's servers include an automated back-up procedure on a daily basis. The Company's office is equipped with fire detectors, fire extinguishers and other applicable measures for the case of consummation of a nature disaster.

System Control

Access to the Company's database is highly restricted in order to ensure that solely the appropriate prior approved personnel can access the Personal Data. Safeguards related to remote access and wireless computing capabilities are in implemented therein. Employee are required to comply with the Company's password policy when composing a password in order to allow strict access or use related to Personal Data, all in accordance with position, and solely to the extent such access or use is required. There is constant monitoring of the access to the data and the passwords used to gain login access. In addition the Company implement automatic captcha, lock-out mechanism, and disable any saving password program in order to prevent any unauthorised login to the Company's servers by the means of password guessing. Electronic procedures in order to terminate an inactive session are also in use by the Company.

Data Access Control
There are restrictions in place to ensure that the access to the Personal Data is restricted to employees which have a permission to access it. The Personal Data shall not be accessed, modified, copied, used, transferred or deleted without specific authorization. The access to the Personal Data, as well as any action performed involving the use of the protected health information requires a password and user name, which is routinely changed, as well as blocked when applicable. The user password is fully encrypted. Each employee is able to perform actions solely according to the permissions determined by the Company. Each access is logged and monitored, and any unauthorized access is automatically reported. Further, the Company has ongoing review of which employees' have authorizations, to assess whether access is still required. Company revokes access immediately upon termination of employment. Authorized individuals can solely access Personal Data that is established in their individual profiles.

Device and Media Controls
Any use of an electronic media shall be done according to the Company's electronic media policy to prevent loss of any Personal Data. Prior to any re-use of electronic media, all Personal Data stored in such electronic media is being transferred to the Company's servers and deleted from the electronic media. The Company monitoring and recording of the movement of each electronic media stored with protected health information. The disposition of any electronic-media is done according to the Company's electronic-media disposition policy.

Organizational and Operational Security
The Company invests a multitude of efforts and resources in order to ensure compliance with the Company's security practices, as well as continuously provides employees on-going training and periodic updates regarding Company's security procedures. The Company strives to raise awareness to the risk involved in the processing of protected health information. In addition, the Company implemented applicable safeguards for its hardware and software, including web content filtering, firewalls and anti-virus software ("**Protection Measures**") on applicable Company hardware, software or employee's computer, in order to protect against virus, worms, Trojan identifications or any other malicious software. The Protection Measures cannot be deactivated by any user other than the Company's cyber security officer and according to the Company's policies.

Transfer Control
The Company does not transfer any Personal Data outside of the Company's cloud servers. All transfer of Personal Data between the client side and the Company's servers is protected using encryption safeguards such as L2TP, IPsec (or equivalent protection), as well as encryption of the protected health information prior to the transfer of any protected health information. Furthermore, the destruction of Personal Data following termination of the engagement is included within the contract between the parties. In addition, to the extent applicable, the Company's business partners execute an applicable Data Processing Agreement, all in accordance with applicable laws.

Data Retention
Personal Data is retained for as long as needed to provide the services or as required under applicable laws. Individuals may request data deletion, however this request is not absolute and is limited, all as detailed in the Company Privacy Policy.

Job Control
Company's employees are required to execute an employment agreement which includes confidentiality provisions as well as applicable data protection provisions binding them to comply with the Company's policies, in particular the computer security policy. In addition, employees undergo a screening process applicable per regional law. In the event of a breach of an employee's obligation or non-compliance with the Company's policies, the Company includes repercussions to ensure compliance with the policies all

according to the Company's sanction policy. In addition, prior to the Company's engagement with third party contractors, the Company reviews such third party's security policies, specifically their information data security policies to ensure it complies with the Company's standard for data security protection. Third party contractors may solely access the Personal Data as explicitly instructed by the Company.