DATA PRIVACY POLICY

Burjeel Holdings PLC

1. General Provisions

This data privacy policy (hereinafter the "Policy") of Burjeel Holdings PLC including its affiliates and subsidiaries ("Burjeel") has been developed in accordance with Abu Dhabi Global Market ("ADGM") Data Protection Regulations 2021, as amended from time to time ("DPR") and the data protection laws of other applicable jurisdictions, for which we note the following key definitions and based on which Burjeel will be obligated to comply with the DPR in relation to all Personal Data for which it is a Controller, that it is Processing on behalf of another Controller and where it is a joint Controller:

a. Board: means the Burjeel's Board of Directors.

b. **CDP:** means the commissioner for data protection, being Burjeel's Chief Information Security Officer or such other person appointed by Burjeel's Board in accordance the DPR to be the head of the Office of Data Protection.

c. **Controller**: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

d. **Data Subject**: means an identified or identifiable living natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

e. **International Organisation:** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

f. **Personal Data**: means any information relating to a Data Subject.

g. **Processing**: means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

h. **Processor**: means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

i. **Services**: means our websites, mobile applications, and other online or digital platforms, as well as any services we provide to Data Subjects.

This Policy applies to the websites, mobile application, and in-person interactions and services provided by Burjeel and its operating division(s) ("**we**," "**us**," or "**our**"), where "**Operating Division(s)**" shall mean the operating divisions, subsidiaries, branches, business divisions, entities operated or managed by Burjeel or its subsidiaries or branches, now or in future, in the United Arab Emirates, Oman, India, Saudi Arabia or elsewhere internationally.

Burjeel is the Controller of the Personal Data with regard to the Processing disclosed in this Policy. This Policy applies to individually identifiable Personal Data that we Process about a Data Subject for any purposes, including in relation to obtaining medical care through our Services (information related to your healthcare is also referred to as "**Protected Health Information**" or "**PHI**"). Such Personal Information is subject to laws and regulations of the applicable jurisdiction where it is Processed, including the UAE as applied in the relevant Emirate, including the UAE Federal laws and the laws and regulations of the Department of Health Abu Dhabi, the Dubai Health Authority and the UAE Ministry of Health ("**UAE Laws**").

The UAE Laws and other applicable jurisdictions' data protection laws dictate how Company and its Operating Division(s) can use and share your Personal Data and PHI and also describes your rights with respect to this information. This Policy supplements these laws and regulations. If there is ever any conflict between this Policy and the data protection laws of other jurisdictions, UAE Laws, Department of Health Abu Dhabi, Dubai Health Authority or UAE Ministry of Health regulations, such other laws will apply.

2. Collection of Information

Depending on the nature of your interactions with us, Burjeel and its Operating Division(s) collect some or all of the following types of Personal Data (including PHI):

a. Contact information, such as your full name, email address, mobile phone number, and address;

b. Specific location data;

c. Profile including family member details maintained in the mobile application;

d. Payment information, such as your credit card number, expiration date, and credit card security code;

e. Personal health information, including information about your diagnosis, previous treatments, general health, and health insurance; and

f. Any other information you may provide to us.

We combine such Personal Data with information we already have collected about the Data Subject(s).

3. Cookies and Tracking Tools

We also collect certain Personal Data automatically when the Data Subject uses our Services, such as the Data Subject's computer's Internet Protocol (IP) address, device and advertising identifiers, browser type, operating system, Internet service provider, pages that you visit before and after using the Services, the date and time of your visit, information about the links you click and pages you view within the Services, details of transactions carried out through our sites, records, copies and full history of your correspondence through our registered contact methods, the comments on surveys

that we might ask our visitors to complete for research purposes & improvement of services, and other standard server log information.

We use cookies, pixel tags, Local Shared Objects, and similar technologies to automatically collect this Personal Data. Cookies are small bits of information that are stored by your computer's web browser. Pixel tags are very small images or small pieces of data embedded in images, also known as "web beacons" or "clear GIFs," that can recognize cookies, the time and date a page is viewed, a description of the page where the pixel tag is placed, and similar information from the computer or device of the Data Subject(s). Local Shared Objects (sometimes referred to as "Flash Cookies") are similar to standard cookies except that they can be larger and are downloaded to a computer or mobile device by the Adobe Flash media player. There are different types of cookies, including: (1) first-party cookies, which are set by our website, (2) third-party cookies, which are set by a third-party when you visit our website, (3) session cookies, which will expire at the end of your browser session when you close the browser window, and (4) persistent cookies, which last for longer than your browser session. You can choose not to allow some types of cookies, but please note that blocking some types of cookies may negatively impact your experience on our website and the services we are able to offer.

We use the Personal Data collected from cookies and tracking tools for the following purposes: to provide website functionality, to understand and tailor website performance, to serve targeted advertising based on your interests, to address and fix technical problems, and to improve our Services. The device or browser settings of the Data Subject may permit the Data Subject(s) to control the collection of this technical data.

Web Analytics Tools: We use on our sites Facebook Pixel & Google Analytics, for the purpose of understanding the Data Subjects' use of our websites. We use Google Analytics to better understand how our visitors interact with our websites. You can learn about Google Analytics' currently available opt-outs at https://tools.google.com/dlpage/gaoptout/.

4. Required Google Play Disclosures for Certain Health Apps

For our application to be available in the Google Play store, we must provide to Google certain Personal Data, as described below.

a. The mobile application interacts with and uses your device's microphone only if you provide permission.

b. The application accesses, collects, uses, and shares Personal Data as stated below in the section titled, "Use of Information."

c. The application permits the Data Subject to conduct telehealth appointments.

5. Information Received from Third-Party Services

If the Data Subject accesses the Services from an advertisement on a third-party website, application, or other service (a "**Third-Party Service**") we may automatically receive Personal Information from the owner of the Third-Party Service related to the Data Subject or that advertisement, using cookies, pixels, or other tracking tools.

6. Sources from which we receive Personal Data

In connection with Services that involve medical treatment, we collect medical records from the Data Subject's past, current, and future health care providers (to the extent applicable). This may include Personal Data about diagnosis, previous treatments, general health, laboratory and pathology test results and reports, social histories, any family history of illness, and records about phone calls and emails related to illness.

As described above, we automatically collect certain Personal Data about your usage of our Services using cookies and other tracking tools. We also receive Personal Data directly from you when you voluntarily provide it to us (e.g., when you create an account or submit an enquiry form). We also receive Personal Data from other sources, including through third-party services and organizations. We may combine our first-party data, such as email address or name, with third-party data from other sources and use this to contact Data Subjects (e.g. through direct mail). For example, if a Data Subject accesses third-party services, such as Facebook, Google, or Twitter, through the Services to login to the Services or to share information about their experience on the Services with others, we shall collect Personal Data from these third-party services.

7. Use of Information

Depending on our interactions with you, we use the Personal Data we collect for a range of purposes, such as to:

a. Optimize and continuously improve our performance and the user experience;

b. Provide and improve the Services;

c. Give a personalized experience on websites and applications, such as personalizing content, user preferences, and languages;

d. Provide our customer service to you and improve our services. This includes from the time you began using the application, any error messages or codes, the model of the device used and its operating system, and the version of our mobile application that is available. If you use Android devices, we also collect your connection type (cellular or WiFi) information during an error;

e. To send you marketing communications and to serve advertising for our products and services, or those of our affiliates and third parties that we think you might be interested in;

f. Contact Data Subjects and fulfill requests for products, services, and information;

g. Send Data Subjects information about additional clinical services or general wellness from us or

on behalf of our affiliates;

h. Access Personal Data collected by Apple's HealthKit or Google Fit which is integrated with the Health application on your respective mobile device.;

i. Use the device of Data Subjects to temporarily hold copies of documents (e.g. image or a letter) which are deleted when the application is closed;

j. Use the device of Data Subjects to temporarily store identifiers and times for upcoming appointments in the Data Subject's device's storage to detect when the Data Subject arrives for an upcoming appointment. When a Data Subject stops using our mobile application or disables the feature, such identifiers (and location data, Bluetooth data) are removed from the in-application storage;

k. Analyze the use of our Services and user data to understand and improve Services;

l. Conduct research using Personal Data, which may be subject to separate written authorization;

m. For security, safety, compliance, and due diligence purposes.

n. Prevent, detect, and investigate potentially prohibited or illegal activities or activities otherwise in violation of our Terms of Use; and

o. For any other purposes disclosed to the Data Subject at the time we collect the Personal Data or pursuant to the Data Subject's consent.

8. Lawful Basis for Processing Personal Data

We Process Personal Data on the following legal bases:

a. Contract: It is necessary for our performance of the contract you have agreed to enter with us for the provision of our Services. If you do not provide your Personal Data to us, we will not be able to carry out our obligations under the terms of the contract.

b. Legitimate Interests: We Process your Personal Data if it is based on our legitimate interests. For example, we may Process Personal Data in reliance on a legitimate interest in the effective and lawful operation of our business, the effective delivery and improvement of our products, Services, and platforms, information security operations, compliance with laws and regulations, compliance with requests for disclosure to law enforcement, courts, and regulatory bodies, and to prevent and detect fraud or suspected fraud. In relation to general inquiry and complaints you send us, our legitimate interest is to provide you with information you have requested and to provide customer support.

c. Consent: Where you have given us consent to do so, we provide you, or permit third parties to provide you, with information about goods or services which we feel may interest you. You have the right to withdraw your consent.

d. Legal Claims: We may need to Process your Personal Data to defend or establish a legal claim (for example, claims relating to the provision of our Services).

9. Sharing of Information

We are committed to maintaining the trust of our patients, employees and other third parties, and we want them to understand when and with whom we shall share the Personal Data we collect.

I. *Authorized third-party vendors and service providers*

We may share Personal Data with third-party vendors and service providers that help us with specialized services, including billing, payment processing, providing medical advice for telemedicine services, management and hosting of telemedicine services, customer service, email deployment, business analytics, marketing (including but not limited to advertising, attribution, deep-linking, direct mail, mobile marketing, optimization and retargeting) advertising, performance monitoring, hosting, and data processing. These third-party vendors and service providers shall not use such Personal Data for purposes other than those related to the services they are providing to us.

II. *Legal, judicial, and law enforcement purposes*

We shall disclose Personal Data to respond to court orders, legal process, law enforcement requests, legal claims or government inquiries, and to protect and defend the rights, interests, health, safety, and security of Burjeel and its operating division(s), patients, users, or the public.

III. *Business Transfers*

If we sell any of our businesses or assets, apply for loans, or open bank accounts, we may disclose your Personal Data to the prospective buyer, lender or bank, as the case may be, as part of certain due diligence processes. If part of our business is acquired by a third party, we may include Personal Data as part of that transaction. We may also share your Personal Data if there is a change to our corporate structure. We may share Personal Data and other information with others as they conduct diligence of our corporate changes.

IV. *Other Reasons we Describe From Time to Time*

With the Data Subjects' consent or at their direction, we shall share Personal Data for any other purposes disclosed at the time we collect the Personal Data or pursuant to the consent or direction obtained.

V. *Public Activities and Third-Party Sites*

If Data Subject(s) chooses to engage in public activities on the third-party sites that we link to, Data Subject(s) should be aware that any information shared there can be read, collected, or used by other users of these sites and forums. Data Subject(s) should use caution in disclosing Personal Data while participating in these areas. We are not responsible for the Personal Data submitted in public areas.

No Personal Data provided by patients during medical consultations or requests for medical appointments is ever used for marketing purposes.

10. Choices

We do not share Protected Health Information with third parties for their own direct marketing purposes.

You can opt out of receiving our marketing emails. To stop receiving our promotional emails, you can follow the instructions in any promotional message you get from us. Even if you opt out of getting marketing messages, we will still send you transactional messages. These include responses to your questions and appointment reminders.

You can control certain location tracking tools. To control the collection of your precise location on your mobile device, you can adjust the settings on your mobile device, such as by disabling location services and turning off the Bluetooth and Wi-Fi. To learn more about mobile location analytics and certain options with respect to mobile location analytics, visit https://smart-places.org.

You can control cookies and tracking tools. Data Subject(s) may be able to refuse or disable cookies by adjusting your web browser settings. Because each web browser is different, please consult the instructions provided by your web browser (typically in the "help" section). Data Subject(s) may need to take additional steps to refuse or disable Local Shared Objects and similar technologies. For example, Local Shared Objects can be controlled through the instructions on Adobe's Setting Manager page. If Data Subject(s) chooses to refuse, disable, or delete these technologies, some of the functionality of the Services may no longer be available. You should make these choices on each devices and each browser you use to access our Services.

Opt-out. To opt-out of interest-based advertising across browsers and devices from companies that participate in the Digital Advertising Alliance or Network Advertising Initiative opt-out programs, please visit their respective opt-out tools at visit www.aboutads.info/choices and https://optout.privacyrights.info. You may also be able to opt-out of interest-based advertising through the settings within the mobile app or your mobile device, but your opt-out choice applies only to the browser or device you are using when you opt-out, so you should opt-out on each of your browsers and devices. If you opt-out, you may still receive ads, but they may not be as relevant to you and your interests, and your experience on our Services may be degraded.

Do-Not-Track Signals and Similar Mechanisms. Some web browsers transmit "do-not-track" signals to websites. Because of differences in how web browsers incorporate and activate this feature, it is not always clear whether users intend for these signals to be transmitted, or whether they even are aware of them. We currently do not act in response to these signals.

11. Privacy Rights of Data Subjects

Depending on where you live or interact with us, you may have any or all of the following privacy rights, based on applicable data privacy law, regarding your Personal Data (each of which are subject to various exceptions and limitations):

The right to be informed: You have the right to be provided with clear, transparent and easily understandable information about how we Process your Personal Data and your rights. This is why we are providing you with the information in this Policy.

The right of access: You may have the right to obtain access to your Personal Data (if we are Processing it) and certain other disclosures similar to those provided in this Policy. This is so you are aware and can check that we are Processing your Personal Data in accordance with applicable data privacy law.

The right to rectification: You may be entitled to have your Personal Data corrected or updated if it is inaccurate or incomplete.

The right to erasure: You may be entitled to request the deletion or removal of your Personal Data where there's no compelling reason for us to keep using it. This is not a general right to erasure; there are exceptions.

The right to restrict Processing: You may have rights to 'block' or suppress further Processing of your Personal Data. When Processing is restricted, we can still store your Personal Data. We keep lists of people who have asked for further use of their Personal Data to be 'blocked' to make sure the restriction is respected in the future.

The right to data portability: You may have rights to obtain and reuse portable copies of your Personal Data for your own purposes across different services and platforms. This may include medical records.

The right to object: You may have the right to object to certain types of Processing, in particular Processing based on our legitimate interests. You may also be entitled to object at any time to your Personal Data being used for direct marketing purposes (including profiling related to such direct marketing).

The right to refuse or withdraw consent: You may have the right to refuse to provide, or to withdraw, your consent to Processing of your Personal Data at any time with effect for future Processing.

If any or all of the above privacy rights apply to you based on applicable privacy law, you can submit a request regarding your Personal Data to privacy@burjeelholdings.com.

If you are not satisfied with our response to your complaint or believe our Processing of your Personal Data does not comply with applicable data privacy law, you can make a complaint to a supervisory data protection authority or regulator.

12. International Transfer of Information Outside ADGM

Personal Data will primarily be Processed within the ADGM, but it may also be transferred outside of the ADGM or to an International Organisation in accordance with applicable data privacy laws. We can transfer Personal Data outside of the territory from which it was initially collected in the following circumstances:

a. without specific regulatory authorisation, where the applicable regulator has determined that the receiving jurisdiction, specified sectors within the receiving jurisdiction or an International Organisation has an adequate level of protection of Personal Data ("**Adequacy Jurisdictions**");

b. without specific regulatory authorisation, where the transferring company (whether Controller or Processor) determines that the receiving jurisdiction, specified sectors within the receiving jurisdiction or an International Organisation has provided the appropriate safeguards and that it has effective legal remedies available for Data Subjects (this is limited to specific circumstances, such as contracts between public authorities, binding corporate rules within an international organisation, adopted standard contractual clauses, an approved code of conduct or an approved certification mechanism);

c. with specific regulatory authorisation, the transferring party and receiving party may enter into certain contractual provisions governing the appropriate safeguards in place regarding the Personal Data; or

d. upon one of the following conditions applying to the transfer:

    1. the Personal Data has been requested from a public authority which has jurisdiction over the Controller or Processor;
    2. the Data Subjects have consented to the transfer, having been informed of the possible risks;
    3. the transfer is necessary for the performance of a contract between the relevant Data Subject and the Controller (or the implementation of pre-contractual measures requested by the Data Subject);
    4. the transfer is necessary for the performance or conclusion of a contract in the interest of the Data Subject between the Controller and another person;
    5. the transfer is necessary for reasons of public interest (in accordance with applicable privacy law) or to protect the vital interests of the Data Subject or another person; or
    6. the transfer is required by law enforcement agencies in the applicable jurisdiction or is necessary for the establishment, exercise or defence of legal claims.

13. Security

We use measures designed to protect Personal Data including PHI from loss, theft, misuse, and unauthorized access, disclosure, alteration, and destruction in accordance with applicable UAE Laws.

We use measures designed to protect other information from loss, theft, misuse, and unauthorized access, disclosure, alteration, and destruction. However, Data Subjects should understand that no data storage system or transmission of data over the Internet or any other public network can be guaranteed to be 100% secure.

14. Third-party Links and Content

Some of the Services may contain links to content maintained by third parties that we do not control. We are not responsible for the privacy practices of these third parties, and the information practices of these third parties are not covered by this Policy.

15. Policy Approval

This Policy shall be reviewed and approved by Burjeel's Board. This Policy shall be effective from the date of approval by the Board. All amendments to this Policy will be done in compliance with applicable laws and will require approval by the Board. The Chief Information Security Officer from the Information Technology Department (together with the Compliance Officer) is the custodian of this Policy.

16. Documentation and Regular Review

Organization Scope	Burjeel
Parent Process	Compliance Program
Document owner	Compliance Officer
Approved by	Burjeel Board of Directors
Initial date published	February 10, 2023
Document effective date	February 10, 2023
Document updated as per	-
Contact person	Compliance Officer
Version	1.0

Burjeel's Compliance Officer shall periodically evaluate the effectiveness of this Policy, and review and revise it as necessary, including to reflect any changes required by applicable laws. You can direct any suggestions for improvements to this Policy to Burjeel's Compliance Officer at cs@burjeelholdings.com.