PRIVACY POLICY
HEALTH TECH SOLUTIONS LLC (Tibbit)

This Privacy Policy (the "Policy") sets out the procedure for the collection, systematization, storage, modification, supplementation, use, provision, transfer, depersonalization and destruction of personal data carried out by HEALTH TECH SOLUTIONS LLC in providing and operating the Tibbit service.

The Policy applies to the Tibbit website, the Tibbit mobile application, personal accounts, software modules and other related digital interfaces through which the User accesses Tibbit functions (collectively, the "Tibbit Service"). The Policy applies to patients, their legal or authorized representatives, website visitors, mobile application users, employees and other representatives of medical organizations and other organizations using the Tibbit Service.

For the purposes of this Policy, HEALTH TECH SOLUTIONS LLC is referred to as "Tibbit" and, within the scope of the processing it actually carries out, acts as the owner and/or operator of the personal data database. A medical organization may independently act as the owner and/or operator of the personal data that it receives, creates and uses in providing medical services. The allocation of responsibilities between Tibbit and a medical organization is determined by the legislation of the Republic of Uzbekistan, the contract and the actual purposes of processing.

Tibbit is a technology service and does not replace a medical organization, an attending physician, a medical consultation, a diagnosis or a prescription. Consent to the processing of personal data does not replace informed voluntary consent to medical intervention or other documents that a medical organization is required to obtain in accordance with the law.

The Policy does not govern the processing of data on third-party websites and services to which the User navigates via an external link, where such services independently determine the purposes and means of processing. Before using a third-party service, the User is advised to review its privacy documents.

Use of the publicly available functions of Tibbit means that the User has read this Policy. Where the law or Tibbit functionality requires consent for a specific operation, such consent is requested separately. Use of the Tibbit Service in itself is not deemed consent to the processing of medical data, receipt of advertising, access to geolocation or any other processing that requires a separate expression of the User's will.

1. User Information Received and Processed by Tibbit

1.1. The following basic terms are used for the purposes of the Policy:

1.1.1. Personal data means information recorded on an electronic, paper or other tangible medium that relates to a specific individual or allows that individual to be identified.

1.1.2. User means an individual who uses the Tibbit Service personally or as a legal or authorized representative of another person, as well as an individual who uses Tibbit on behalf of a medical or other organization.

1.1.3. Medical organization means a clinic, medical center, physician or other person lawfully providing medical services and using Tibbit to organize appointments, maintain medical records and interact with patients.

1.1.4. Consent means a voluntary, specific, informed and verifiable expression of the User's will to the processing of personal data for the stated purposes. For special personal data, Consent is given in writing, including in the form of an electronic document, unless another legal basis for processing is expressly provided by law.

1.1.5. Medical data means information about physical or mental health, the fact of seeking medical care, diagnosis, examination, treatment and other circumstances of the provision of medical care. Such information constitutes special personal data and may constitute medical confidentiality.

1.1.6. Processing of personal data means one action or a set of actions for the collection, systematization, storage, modification, supplementation, use, provision, dissemination, transfer, depersonalization and destruction of personal data.

1.2. The specific scope of data depends on the function used, the User's status, the selected medical organization, the permissions granted and the integrations. Tibbit does not seek to collect data that is not required for the stated purposes.

1.3. Identification data may include surname, first name, patronymic, date of birth, sex, personal identification number of an individual (PINFL), passport or ID card details, citizenship, and a photograph of a document or face, where necessary for identification provided for by law or by the functionality.

1.4. Contact data may include telephone number, email address, residential address and, where necessary, the name and contact details of a legal representative, relative or other contact person specified by the User.

1.5. Account data may include login or telephone number, a hash or other cryptographically protected representation of the password, the User's internal ID, account status, registration date, information about the registration and authorization method, login history, linked devices and profile settings.

1.6. Medical data may include the electronic medical record, diagnoses, complaints, medical history, results of tests and examinations, medical images and documents, prescriptions, information on medicines, allergies and contraindications, vaccinations, medical reports, visits and appointments, as well as information about the physician and the medical organization where the User was served.

1.7. Data on appointments for medical services may include the selected clinic and branch, physician, specialty, service, appointment date and time, appointment comment, appointment status, history of confirmations, cancellations and rescheduling, attendance information and related service notifications.

1.8. Financial and payment data may include the amount, currency, purpose and status of the payment, the date and time of the transaction, the transaction ID, invoice and order identifiers, the token or masked details of a linked bank card, refund information, data on payment via ePOS, and information received from a bank, payment organization or payment system. Tibbit does not ask the User to disclose a CVC/CVV and/or OTP code to Tibbit employees.

1.9. Technical data may include IP address, Device ID and other device or application identifiers, device type, manufacturer and model, operating system, application version, browser, device language, time zone, screen resolution, date and time of access, address of the requested page, referer, User-Agent, ClientID, session and authorization data, activity logs, error reports, and performance and information security data.

1.10. Geolocation data, if the relevant function is actually used and the User has granted system permission, may include current precise geolocation, approximate location and location history. Location history is collected only where this is directly necessary for an operating function and has been separately brought to the User's attention.

1.11. Communications data may include chat messages, attachments, support requests, the content and status of push, SMS and other notifications, the history of communication with the medical organization, reviews, ratings and information on the handling of complaints.

1.12. Consent data may include the fact that Consent was given, its text or version, the type and purpose of Consent, the date and time it was given, the method of confirmation, technical evidence of the expression of will, information on withdrawal and the history of changes to Consent.

1.13. Automatically collected data may include the User's actions in the application and on the website, sections visited, functions used, the sequence of navigation, interface events, application errors, analytics data, cookies and similar technologies, where used. Necessary cookies are used for the operation and security of the website; optional analytics or advertising technologies are used where the required legal basis exists and a choice setting is available.

1.14. Data from third parties may be received from banks and payment systems, state information systems, medical organizations, laboratories, pharmacies, insurance organizations,

integration partners, authorization service providers and other persons with whom the User interacts or from whom the User has initiated or authorized a transfer.

1.15. If the "Garage" module is used in Tibbit, vehicle data may be processed: manufacturer, make and model, state registration number, color, link to the User's profile and history of service appointments. This information is not collected if the module is not activated and not used.

1.16. When the device's system biometric authentication (for example, Face ID, Touch ID or fingerprint) is used, the biometric template is processed by the device's operating system. Tibbit receives only the technical result of whether the check was successful and does not receive the biometric template, unless the User is separately notified otherwise before the relevant processing begins.

1.17. The User must not place data of a third party in Tibbit without a legal basis. By providing data of a representative, relative, patient, employee or other person, the User confirms that they have authority or another applicable basis and must, where possible, notify such person of the processing.

2. Purposes of Collecting and Processing Users' Personal Information

2.1. Tibbit processes only such data as is necessary and proportionate to a specific purpose and does not use it in a manner incompatible with the originally stated purpose without a new legal basis.

2.2. When the Tibbit website is used, data may be processed for the following purposes:

2.2.1. Receiving and processing applications for connecting clinics and organizations, contacting the applicant regarding a submitted application, preparing proposals, contracts and individual terms, and providing information on products, services and rates.

2.2.2. Registration, account creation, identification and authorization of the User, and provision of access to the personal account and its functions.

2.2.3. Processing requests submitted via feedback forms, support requests and other communications, and maintaining a history of interaction with the User or organization.

2.2.4. Processing payments and settlements for Tibbit services, generating payment and accounting documents, and performing contractual and statutory obligations.

2.2.5. Ensuring the security of the website and accounts, preventing unauthorized access, fraud and abuse, and investigating incidents.

2.2.6. Analyzing website usage, fixing errors, improving performance and usability, and maintaining statistics based on minimized, aggregated or depersonalized data where possible.

2.2.7. Sending service notifications; sending marketing and informational messages only where separate Consent has been given, if such Consent is required.

2.3. When the Tibbit mobile application is used, data may be processed for the following purposes:

2.3.1. Registration, account creation, identification, authentication and verification of the User's identity as provided for by the functionality.

2.3.2. Creating and maintaining a patient profile, and linking the profile with a representative, a medical organization and medical documents where the relevant authority and grounds exist.

2.3.3. Searching for clinics, branches, physicians and medical services; online booking; viewing, confirming, rescheduling and cancelling appointments; building a visit history.

2.3.4. Receiving, storing and displaying the User's medical information, including the electronic medical record, test and examination results, prescriptions and medical reports, within the scope of the User's Consent, the authority of the medical organization and other legal grounds.

2.3.5. Organizing communication between the patient and the medical organization, operating chat and support, and sending push and other service notifications about bookings, appointments, documents, payments and status changes.

2.3.6. Collecting and displaying reviews and ratings of physicians, services and medical organizations, moderating materials and handling complaints.

2.3.7. Initiating and supporting payment for medical services through an engaged payment service provider, storing transaction history, operating the linked card token and processing refunds.

2.3.8. Personalizing application content and displaying relevant services, offers, banners and other content based on the User's settings, usage history and Consent, where required.

2.3.9. Ensuring the security of the application and account, preventing fraud, diagnosing errors, technical monitoring and analyzing the use of functions in order to improve them.

2.3.10. Using geolocation to display the nearest medical organizations, determine the region, build a route or perform another clearly indicated function, only when the device permission is enabled and to the extent necessary for such function.

2.4. The common purposes of processing for the website and the mobile application are: providing and operating Tibbit; performing contracts and taking steps at the User's request prior to entering into a contract; handling requests; technical support; information security; fraud prevention; improving the quality of the Service; maintaining statistics and analytics; complying with legal requirements; and protecting the rights and legitimate interests of Users, Tibbit, medical organizations and partners.

2.5. The processing of medical data and information about health status is treated as a separate purpose. Such data is processed to organize and document medical care, to give the User access to their medical information and to ensure lawful data exchange with the selected medical organization.

2.5.1. Medical data is processed on the basis of separate written Consent, including in the form of an electronic document, an instruction or legal basis of the relevant medical organization, and/or in other cases expressly provided for by the legislation of the Republic of Uzbekistan.

2.5.2. Medical data is not used for third-party advertising, sale, determination of insurance rates, discrimination against the User or training of artificial intelligence models, unless the data has been properly depersonalized, or the User has given separate specific Consent and the processing is permitted by law.

2.6. Payment data is processed to initiate, confirm and record transactions and refunds, prevent fraud, handle claims and comply with legal requirements. Tibbit does not provide banking or payment services unless expressly stated otherwise by the license and terms of the relevant service; payment is executed by a bank or payment service provider.

2.7. Technical and automatically collected data is used for operability, compatibility, security, diagnostics, abuse prevention, quality measurement and development of Tibbit. For statistics and research, Tibbit seeks to apply aggregation, pseudonymization or depersonalization.

2.8. Communications data is used to fulfil requests, support appointments and payments, confirm actions, monitor quality, resolve disputes and ensure security. The content of medical communications receives the same level of protection as medical data.

2.9. The legal bases for processing may be: the User's Consent; the need to perform a contract to which the User is a party, or to take steps at the User's request prior to entering into a contract; performance of obligations of Tibbit or a medical organization established by law; protection of life, health, rights and legitimate interests in cases provided for by law; and other grounds expressly provided for by the legislation of the Republic of Uzbekistan.

2.10. Advertising and marketing messages are sent on the basis of the User's separate choice. Opting out of such messages does not restrict the core medical and service functions, but does not stop mandatory transactional, security and other service notifications.

2.11. Tibbit does not make decisions that produce legal consequences for the User or otherwise significantly affect the User's rights solely on the basis of automated processing, except in cases of written Consent, the need to perform a contract or other grounds provided for by law. Where such a mechanism is used, the User is provided with information on how the decision is made and an opportunity to object.

3. Processing Conditions, Sources, Retention Periods and Transfer to Third Parties

3.1. Tibbit processes data in accordance with this Policy, Consents, contracts, function settings, internal regulations and the legislation of the Republic of Uzbekistan. Processing may be automated, non-automated or mixed.

3.2. The sources of data are:

3.2.1. The User themselves: during registration, completion of the profile and forms, uploading documents, booking, payment, contacting support, chatting, submitting a review and using other functions.

3.2.2. Medical organizations, physicians, laboratories, diagnostic centers, pharmacies and other participants in medical care, to the extent necessary to provide services, maintain records and give the User access to information.

3.2.3. Banks, payment organizations, payment systems and ePOS providers, with respect to the status, identifiers and other transaction parameters, the card token, refunds and payment security checks.

3.2.4. State information systems, where an integration and a legal basis exist and the established procedure for inter-system exchange is observed.

3.2.5. Integration partners, authorization services, communications providers and other counterparties, when the relevant function is used and within the scope of the necessary exchange.

3.2.6. The User's device, browser and application, automatically, in the form of technical, analytical, session and permitted geolocation data.

3.3. Where data is not received from the User, Tibbit takes into account the source, purpose, legal basis and restrictions established by the transferring party. A medical organization is responsible for the lawfulness and accuracy of the data it creates or transfers to Tibbit in the course of its activities; Tibbit is responsible for the lawfulness and security of the processing that it independently determines and carries out.

3.4. Tibbit records the giving and withdrawal of Consent in a manner that confirms the identity or account, the text and version of the Consent, the purpose, the method of confirmation, and the date and time. Withdrawal takes effect for the future and does not render unlawful the processing carried out before it was received.

3.5. Data is stored no longer than necessary for the relevant purpose, the term of the Consent, the performance of the contract, protection against claims and fulfilment of obligations established by law. Where a different period is established for a specific category by law, contract or mandatory regulations, that period applies.

3.5.1. Website applications and correspondence with a prospective client that did not result in a contract are stored for up to three years after the last substantive interaction, unless the User has requested earlier deletion and there is no other legal basis.

3.5.2. Account and profile data and booking history are stored for the life of the account and for up to three years after its closure or the last legal relationship, unless longer storage is required for medical records, dispute resolution or compliance with the law.

3.5.3. Medical data and documents are stored for the period necessary to provide access and work with the medical organization, and thereafter for the mandatory retention period for medical records established by law and the rules of the relevant medical organization. Withdrawal of Consent does not entail the destruction of data that the medical organization or Tibbit is required by law to retain.

3.5.4. Payment information is stored for the periods established by legislation on payments, accounting and tax records, the rules of the payment provider and the periods for handling claims. The card token is deleted or deactivated after the card is unlinked, unless its further storage is required for an incomplete transaction, refund, dispute or security.

3.5.5. Ordinary technical and analytics events are generally stored for up to twenty-four months. Security, authorization and significant-action logs may be stored for up to three years or longer if necessary to investigate an incident, protect rights or comply with the law.

3.5.6. Support requests, chats and other communications are stored for up to three years after the request is closed or the relevant interaction ends, and medical messages are stored under the rules for medical data.

3.5.7. Current geolocation is processed within the scope of an active function request. Geolocation history, if the relevant function is enabled, is stored for no more than twelve months, unless the User is informed of a different necessary period before collection or longer storage is required by law.

3.5.8. Evidence of Consent and its withdrawal is stored for the entire period of the relevant processing and for up to five years after it ends to confirm the lawfulness of actions, unless a different period is established by law or by a dispute.

3.5.9. Backup copies may be retained for up to ninety days after data is deleted from the active system. During this period, data from a backup copy is not used for ordinary operations and is deleted upon scheduled overwriting, unless its retention is required by law or for an incident investigation.

3.6. Upon achievement of the purpose, expiry of the period, withdrawal of Consent or the occurrence of another ground provided for by law, data is destroyed or irreversibly depersonalized, unless there is an obligation to continue storing it. Deletion of a medical record may be replaced by restricting access, archiving or making a corrective entry where preservation of the document history is mandatory.

3.7. Tibbit ensures confidentiality and transfers data to third parties only where there is Consent, a need to perform a function selected by the User or a contract, a lawful instruction from a medical organization, or another ground provided for by law.

3.8. Recipients of data may include:

3.8.1. Medical organizations selected by the User, their branches, physicians and authorized employees, for booking, medical care, record keeping, settlement and communication. Access is granted with regard to roles, authority and medical necessity.

3.8.2. The User's legal or authorized representatives and recipients designated by the User, within the scope of the Consent, power of attorney, law or access settings.

3.8.3. Banks, payment organizations, payment systems, acquirers, issuers, ePOS providers and anti-fraud services, to carry out, confirm, refund and protect payments.

3.8.4. Providers of hosting, storage and backup, cloud infrastructure, technical support, information security and development, to the extent necessary and subject to confidentiality and data protection terms.

3.8.5. Telecom operators and providers of SMS, email, push notifications and support services, to deliver messages and handle requests.

3.8.6. State authorities, courts and other authorized persons, upon a lawful request, within their competence and the established procedure.

3.8.7. Integration partners, state information systems and authorization services, for the function used by the User and to the minimum extent necessary.

3.8.8. Auditors, lawyers, insurers and other professional advisers, where they are bound by confidentiality and it is necessary to protect rights or comply with the law.

3.8.9. A successor or acquirer of the Tibbit business, in the event of reorganization, sale or transfer of the relevant part of the business, provided that data protection obligations are assumed and notification is given in cases provided for by law.

3.9. Analytics and marketing providers primarily receive aggregated, depersonalized or pseudonymized information. Medical data is not transferred to them for their own advertising purposes. Transfer of identifying data for marketing is permitted only with separate Consent and a legal basis.

3.10. Full bank card details and the CVC/CVV code are processed in the secure interface of the bank or payment provider. Tibbit may receive the token, masked number, expiry date, card type and transaction parameters necessary to display the linked payment method and support the transaction.

3.11. Cross-border transfer is carried out where there is a legal basis, subject to the requirements for protecting the rights of data subjects and the restrictions of the legislation of the Republic of Uzbekistan. Before transfer, the nature of the data, the recipient's country, and contractual and technical safeguards are taken into account; where necessary, separate Consent is requested.

3.12. Categories of data that, in accordance with the law, must be stored on the territory of the Republic of Uzbekistan are stored in the Republic of Uzbekistan. Databases subject to registration in the State Register of Personal Data Databases are registered in the established manner.

3.13. Tibbit may generate depersonalized and aggregated data for statistics, research, reporting, development and quality assessment of the Service. Depersonalization is performed so that a specific User cannot be identified without additional information. Any additional information allowing the link to be restored, if it exists, is stored separately and protected.

4. Modification and Deletion of Personal Information, Access to It and User Rights

4.1. The User has the right to receive information about the processing of their personal data, including the fact and legal basis of processing, the purposes, methods, scope of data, sources from which it was obtained, processing and retention periods, categories of recipients, any intended or completed cross-border transfer, and the procedure for exercising their rights.

4.2. The User has the right to access their data and obtain a copy of it in the form provided by Tibbit and the law, provided that this does not violate the rights and legitimate interests of other persons, medical confidentiality in respect of third parties, the secrecy of investigation, or commercial or other secrets protected by law.

4.3. The User has the right to demand the modification or supplementation of inaccurate, incomplete, outdated or unlawfully obtained data, submitting supporting documents where necessary. Profile data may be edited in the interface where this option is provided.

4.4. In medical records, a correction may be made by adding a new or corrective entry while preserving the history of changes, the author and the time of the operation. Tibbit may not, at the User's request, change a medical diagnosis or report without the involvement of the medical organization or specialist who created the entry.

4.5. The User has the right to withdraw Consent in whole or in part by the same or another available method that allows the withdrawal to be confirmed, including via the application settings, the support service, or a written or electronic request. Individual Consents, including marketing and geolocation, may be managed independently.

4.6. The User has the right to demand temporary suspension or restriction of processing, blocking or destruction of data where the conditions of processing have been violated, the purpose has been achieved or there is no legal basis, taking into account mandatory retention periods and the rights of the medical organization.

4.7. The User has the right to opt out of advertising messages via an unsubscribe link or setting, and to object to processing based on the relevant Consent. Service notifications necessary for security, bookings, payments or performance of the contract may continue to be sent.

4.8. The User has the right not to be subject to a decision with legal or other significant consequences made solely by automated means, except in cases provided for by law, and to receive an explanation and submit an objection to such a decision.

4.9. The User has the right to appeal the actions or inaction of Tibbit to the authorized state body in the field of personal data or to a court, and to use other means of protection provided for by the legislation of the Republic of Uzbekistan.

4.10. To exercise a right, the User submits a request via the support form provided in Tibbit or using the contacts published in the "Contacts" section of the official Tibbit website. The request should state the name, the preferred method of reply, the account or other identifier, the substance of the demand and information enabling the relevant data to be located.

4.11. If there are reasonable doubts as to the identity or authority of the applicant, Tibbit may request the minimum necessary confirmation. Identification documents are used solely to verify the request and are protected in accordance with this Policy.

4.12. A request is considered within the periods established by the legislation of the Republic of Uzbekistan. If the provision of information is lawfully restricted or the demand is refused, Tibbit states the grounds and the appeal procedure; notice of refusal to provide information about processing is sent to the User in writing within ten days.

4.13. If data has been transferred to recipients, Tibbit, in cases provided for by law, notifies them of the modification, restriction or destruction of the data, unless such actions are impossible or disproportionate. When transferring personal data to a third party, Tibbit notifies the User thereof in writing within three days, except where such notification is not required under the law.

4.14. The rights of a minor User, or a User who is legally incapacitated or has limited legal capacity, are exercised by that User and/or their legal representative in accordance with age, the scope of legal capacity and the law. Consent to the processing of personal data and consent to medical intervention are separate expressions of will and are executed separately where required.

4.15. Withdrawal of Consent or deletion of mandatory data may make registration, access to the electronic medical record, booking, payment or another function impossible. Before fulfilling the request, Tibbit informs the User of significant consequences if they are not obvious.

5. Measures Applied to Protect Users' Personal Information

5.1. Tibbit takes legal, organizational and technical measures aimed at protecting data against unlawful or accidental access, destruction, modification, blocking, copying, provision, dissemination and other unlawful actions.

5.2. Depending on the risk and applicability, such measures include: role-based and need-to-know access control; identification and authentication; password protection; encryption of transmission channels and certain data sets; activity logging; backup; anti-virus and network protection; vulnerability and incident monitoring; disaster recovery; counterparty due diligence; employee training and confidentiality undertakings.

5.3. Access by employees of a medical organization to patient data is determined by the medical organization and by Tibbit technical roles. The medical organization must promptly restrict access for dismissed persons or persons who have lost their authority and must not allow data to be viewed other than for official and medical necessity.

5.4. Tibbit maintains logs of authorization, viewing and modification of significant data to the extent necessary for security, audit, confirmation of actions, handling of complaints and protection of medical confidentiality. Logs are protected against unauthorized modification and are accessible to a limited number of persons.

5.5. When engaging a processor or other counterparty, Tibbit establishes requirements regarding the purpose, scope, period, confidentiality, security, return or destruction of data, and monitors compliance within the limits of the contract and the law.

5.6. Upon detecting an incident, Tibbit takes measures to contain it, assess its consequences, preserve evidence, restore security and notify Users, medical organizations and state authorities in the cases and manner provided for by law.

5.7. The User must keep their password, confirmation codes and device access confidential; not transfer their account to another person; use up-to-date software; and immediately report a suspicious login, loss of a device or possible compromise of data.

5.8. No method of transmission or storage eliminates risk entirely. Tibbit maintains protective measures taking into account the nature of medical and other data, available technologies, the likelihood and severity of possible harm and the requirements of the law, and regularly reviews their adequacy.

6. Amendments to the Privacy Policy. Governing Law

6.1. Tibbit may amend the Policy as the Service develops, as the scope and purposes of processing change, as integrations are connected, or as security or legal requirements change. The

new version is published on the official website and/or in the Tibbit application and applies from the stated effective date.

6.2. Tibbit notifies Users, by available means and before application where required, of material changes affecting the purposes, categories of medical data, the range of recipients or the User's rights. If Consent is required for new processing, such processing does not begin until that Consent is obtained.

6.3. The User is advised to periodically check the current version. Continued use of functions for which separate Consent is not required after the changes take effect means use of Tibbit on the terms of the new version, but does not replace a separate expression of will that is mandatory under the law.

6.4. The Policy and data processing are governed by the legislation of the Republic of Uzbekistan, including Law of the Republic of Uzbekistan No. ZRU-547 "On Personal Data" dated 2 July 2019, Law of the Republic of Uzbekistan No. 265-I "On the Protection of Citizens' Health" dated 29 August 1996, and other regulatory legal acts on personal data, medical confidentiality, payments, and information security and cybersecurity.

6.5. If any provision of the Policy is held invalid or inapplicable, the remaining provisions remain in force. In the event of a discrepancy between the Policy and a mandatory provision of law, the mandatory provision applies.

7. Interaction with Users on Matters of Personal Information Processing

7.1. Questions, requests, complaints, withdrawal of Consent and demands to exercise rights are submitted via the support form in the Tibbit mobile application or personal account, or using the current electronic and postal details of HEALTH TECH SOLUTIONS LLC published in the "Contacts" section of the official Tibbit website.

7.2. To protect data, Tibbit may correspond via a verified telephone number, email address or account, and may request confirmation of identity or of a representative's authority to the minimum extent necessary.

7.3. On matters concerning the content of a medical record, diagnosis, prescription, examination result, access by a specific physician or mandatory retention of medical records, the User may also contact the relevant medical organization directly. Tibbit and the medical organization cooperate to handle the request within their respective authority.

7.4. The current Policy is published on the website and/or in Tibbit.