*The following legal agreement is available for public use at no charge so long as the agreement is sourced back to Bridge along with the copyright information at the end of this agreement template.*

**Privacy Policy**

[Insert name, address and contact information of Provider]

**ACCEPTANCE OF PRIVACY POLICY**

1. This patient portal and its services (“Service”) is provided to you by the healthcare service provider, herein referred to as “Provider”, "we", "us", or "our." The term "you" or "your" refers to the authorized viewers or users of this Service, including but not limited to the patient and their care team.
2. We are committed to maintaining robust privacy protections for the users of our Service. Our Privacy Policy is designed to assist you in making informed decisions when using our Service and help you understand how we collect, use, maintain and protect the information you provide to us via the Service
3. By using this Service by the Provider, you agree to accept the conditions and practices described in this Privacy Policy and consent to the collection and use of information set forth below.
4. If you do not agree with the terms of this Privacy Policy for any purpose, please do not use the self-service features of the Provider’s Service.

**DEFINITIONS**

**Activity Logs**

1. Activity Logs are records of when Protected Health Information (“PHI”) data is generated, accessed, modified, released, deleted, or exported from within the Service.

**Aggregate Data**

1. Aggregate Data is PHI that is: (1) grouped so it does not identify, relate to, describe, be capable of being associated with, connected, or be linked, implicitly or explicitly, , to you as an individual and (2) has names and other identifiers removed or altered. Strictly speaking, Aggregate Data cannot be used to identify you as an individual.

**Authorized User**

1. An Authorized User is you or someone you have legally authorized to access the Service or your PHI.

**De-identified Data**

1. De-identified data is PHI data in which personal identifiers are removed, preventing the ability to determine a person’s identity.

**Dependent**

1. A Dependent is a minor or other individual over whom an Authorized User has legal authority.

**PHI**

1. PHI means Protected Health Information. PHI is stored in an electronic health data application, such as a patient portal or electronic health record software, that can help you compile, administer, and share your health information.

**PHI Data**

1. When you sign up to our Service, you provide and/or you authorize all or some of your Providers, and the authorized employees of the Provider’s business, to have access to your PHI. This information makes up the PHI Data. PHI Data includes Personal Information, De-Identified Data and Aggregate Data. PHI Data might include, but is not limited to the following:
   1. Your name and contact information, such as your address, phone number, or email address;
   2. Your medical history, conditions, treatments, and medications;
   3. Your health plan account numbers, healthcare claims, medical bills, and insurance information;
   4. Demographic information, such as your age, date of birth, gender, and occupation;
   5. Computer information, such as your IP address and "cookie" preferences
   6. The Service may use your PHI Data as described below.

**Personal Information**

1. Personal Information is information or material about you that can be linked to you within reason, such as your name, date of birth, health information, demographic information, and/or other identifiers, as may be defined under U.S. state and federal law. Personal Information may also include but is not limited to your financial details or Social Security Number.

**Security Measures**

1. Security measures can include computer safeguards, intrusion detectors, application controls, secured files, and supplier and vendor employee security training. In addition, the Service supplier and/or Provider may be required by law to notify you, about particular security and data breaches.

**YOUR PERSONAL INFORMATION**

1. Provider and Service will not sell, share or rent the information that is collected via the Service to others except as disclosed in this Privacy Policy.

**Identifiable Health Information**

1. Provider may use any identifiable health information or other data that you voluntarily submit, in order to furnish information, products or services that you wish to request from Provider.
2. Any identifiable health information that you, as a patient, Dependant or legal representative of patient, transmit via the Service will be made accessible to Provider and will become a part of the records maintained by Provider.
3. Service may use your voluntary participation to market special offers and featured services to you, whether from Provider, affiliates, suppliers or vendors, or other third parties, to the extent permitted by applicable law. If you are receiving additional communications and/or special offers, you may revoke your authorization to receive such materials at any time by contacting the Provider.
4. Service also uses your information for communication purposes and to customize your user/browsing experience,and otherwise to respond to your questions and feedback regarding the use of the Service as may be permitted by applicable law.
5. Service may convey your information only with the Provider and the supplier/vendor of the Service to the limited extent permitted by applicable law. We require those suppliers and vendors to comply with all applicable data privacy laws and regulations, including the HIPAA.

1. Service may also use your geographic location to provide you with specific or tailored content to the extent permitted by applicable law.

**Non-Identifiable Health Information**

1. The non-identifiable, aggregated health information the Service collects may be shared with suppliers and vendors and used in the aggregate to generate summary statistics that assist in the analysis of website usage trends, and help to assess what information is valuable, to determine technical design specifications, to design a user-friendly service, and to evaluate system performance or problem areas.

**The Use of Aggregate Data**

1. Service may aggregate and de-identify health information, in accordance with HIPAA, either alone or along with other data to generate anonymous Aggregate Data regarding the user pattern of the Service. Aggregate and de-identified data, without revealing the identity of particular users, is information that describes the habits, treatment plans, usage patterns, other medical record data and/or demographics of users as a group. This data will not identify you, but will be used to assemble statistics on, for example, user demographics and usage patterns of the Service.
2. Service may use Aggregate Data to understand its users and determine what kinds of programs and services most serve their needs. Aggregate Data may also be provided or sold to third parties, including for the purpose of tailoring content to you by third party vendors, suppliers, business partners and/or affiliates, of acquiring a blueprint of our community and services and/or of participating in surveys
3. Provider might report business and customer activities to others, such as investors, auditors and potential business partners. Other than with your express consent, or as permitted or required by law, reports will not include any Personal Information.

**Other Use and Ownership**

1. Service and Provider also reserve the right to share your information collected from the Service, to the extent permitted by applicable law including but not limited to the requirements under HIPAA, and, in the case of identifiable health information, pursuant to the Business Associate Agreement that the supplier/vendor has with Provider.
2. We retain full rights to any information acquired via the Service and may freely collect, use and disclose such information, unless prohibited by this Privacy Policy or applicable law as stated above.

**SECURITY**

1. The Service and Provider will take all steps reasonably necessary to maintain industry standard security levels, and to be in compliance with all applicable state and federal guidelines. Internal audits for security and compliance are conducted routinely and are part of the Service’s development practice. Nonetheless, no Service can guarantee network security or that loss, misuse or alteration to data hosted by or on, or accessed by or through, a website will not occur. While the Service tries to protect and maintain the integrity of your Personal Information against intentional and unintentional corruption, any data you voluntarily disclose to the Service is submitted at your own risk. You agree to hold harmless Provider, if security protocols fail.

**Industry Standard**

1. Service uses industry standards, such as Secure Socket Layers ("SSL") or Transport Layer Security (“TSL”) technology, geo-blocking, two-factor authentication and login security protocols to safeguard against the aforementioned incidences and/or other security breaches. To ensure confidentiality, the information passed between your browser and our system is encrypted with SSL or TSL technology (which covers any messages exchanged using our secure messaging services, as well as your personal information and PHI) to create a protected connection between you and the Service.
2. Service permits limited access to personally identifiable information about you to supplier and vendor employees and third party agents who we reasonably believe need to have access to your information to cater to your needs requested via the Service. In the event that a breach in our security systems occurs by way of unauthorized access or improper disclosure, Provider will notify you of such a breach as may be required by applicable law.

**Access**

1. Service will maintain your information and you can upload, store and access your personal healthcare records and information, including copies of documents, records, images, and information provided by you, by logging into your Service account. Your account information and profile are password-protected.
2. You should first consult Provider if you wish to make any amendments to the information stored in your account.

**MINOR POLICY**

1. We do not have the capacity to monitor or distinguish the age of individuals who access our Service, and so Provider carries out the same Privacy Policy for individuals of all ages. If a minor has supplied Provider with personally identifying information without the express consent of his or her legal representative, the representative should contact Provider to restrict access and remove the information.
2. By using our Service, you certify that you are an Authorized User of sufficient legal age with binding legal and financial obligations for any liability you may incur while using the Service.

***Important Notice Regarding Children under 13 Years of Age***

1. Any information provided via the Service with respect to a minor *under the age of 13* must be formally submitted by the minor's legal representative. To the extent permitted by applicable law, minors may access their identifiable health information through their Provider.

**THIRD PARTY SERVICES**

1. While you use the Service, you may be exposed to services or products offered by other companies that are not part of Service ("Third Party Services"). When taking part in Third Party Services, you are responsible for reviewing any terms and conditions governing such Third Party Services. You understand and agree that the company providing the Third Party Services is solely responsible for the Third Party Services.
2. While the Service may contain links to websites operated by other companies ("Third-Party Sites"), it does not control Third-Party Sites and will not be held accountable for the content of, or any links in, any Third-Party Site. Service does not monitor, review, approve, or make any representations with respect to Third-Party Sites.
3. You acknowledge and understand that Third-Party Sites may contain terms and privacy policies that are different from Provider and all access to Third-Party Sites is at your own risk. Provider and Service are not responsible for or bound by such provisions, and expressly disclaim any liability for them.

**DO NOT TRACK SIGNALS**

1. We do not support Do Not Track ("DNT") under the California Online Protection Act (CalOPPA).

**MODIFICATIONS TO THE PRIVACY POLICY**

1. Provider reserves the right to make amends to the Service and this Privacy Policy at any time. Any changes to Provider’s policies will be expressly communicated to you in advance of its effective date and any information collected before changes are made, will be protected and stored according to the aforementioned provisions.
2. If any part of these conditions shall be deemed invalid, void, or for any reason unenforceable, the provision in question will be deemed severable to the extent of such prohibition or unenforceability without invalidating the remaining conditions hereof. All other provisions set forth in this Privacy Policy shall continue to remain in effect.

By clicking “Agree” below, you confirm that you have read and understood the Privacy Policy and hereby accept all the terms and conditions contained herein.

*Agreement template made available by Bridge Patient Portal LLC. Copyright ©* [*Bridge Patient Portal LLC*](http://www.bridgepatientportal.com)*. All rights reserved.*