

# Notice of Privacy Practices of DatStat, Inc. (“DatStat”)

Last Updated: August 13, 2018

DatStat’s clinical and research-based patient engagement platform, a secure, Internet-based communications and data capture software platform, and related services (collectively, the “Services”) was developed by health researchers, for researchers, doctors, and patients. We understand the importance of the researcher-participant and physician-patient relationships, and the importance of keeping your personal information private. Personal information identifies you as an individual, such as your name, postal address, email address, date of birth and telephone number (“Personal Information”). This Notice of Privacy Practices (the “Privacy Policy”) describes our practices in connection with information that we collect through your use of the Services and through the website from which you access the Services (the “Site”). By using the Services and/or the Site, you agree to the terms and conditions of this Privacy Policy.

Protected Health Information (as defined below) is a part of the Personal Information that we may collect. Protected Health Information that is provided to us or that we otherwise collect is subject to the additional terms and conditions in the “*Protected Health Information*” section below, the terms and conditions of which section will prevail and control if they are inconsistent with or contradictory to the remaining terms and conditions of this Privacy Policy.

## **PERSONAL INFORMATION WE COLLECT FROM RESEARCHERS AND PROVIDERS**

If you are a researcher, physician or other healthcare or medical provider (“Provider”), or an individual who is authorized by a Provider to access and use the Services (“Designee”), we collect Personal Information about you when the Provider subscribes to the Services as well as when you register to use the Services. The Personal Information about Providers and Designees that we collect includes, without limitation, the applicable Provider’s or Designee’s name, specialty, email address, phone number, and business postal address. We do not collect Protected Health Information about Providers or their Designees.

## **PERSONAL INFORMATION WE COLLECT FROM PATIENTS, RESEARCHERS, AND AUTHORIZED CAREGIVERS**

If you are a participant in a health research study, or a patient of a Provider who has subscribed to the Services (“Patient”), we collect Personal Information about you when you register to use the Services and through your or your Authorized Caregiver (as defined below)’s use of the

Services, including when you, your Authorized Caregiver and/or your Provider communicate with each other. If you are an individual authorized by a Patient to use the Services (“Authorized Caregiver”) to communicate with such Patient’s Provider or Research PI / Research Coordinator, we collect Personal Information about you, including, without limitation, your name, email address, phone number and your relationship to the Patient. When communicating with the Provider in using the Services, the Patient, Authorized Caregivers, other Providers and/or their Designees may disclose Personal Information about the Patient, which may include Protected Health Information. We do not collect Protected Health Information about Authorized Caregivers.

## **HOW WE USE PERSONAL INFORMATION**

We may use Personal Information, as follows:

- to enable you to access and use the Services, and if you are a Patient, to access and download your DatStat data.
- to respond to your inquiries.
- to send you important information regarding the Services, changes to our terms, conditions, and policies and/or other administrative information.
- for our business purposes, such as data analysis, audits, developing new products, and enhancing and improving our Site and the Services.
- as we believe to be necessary or appropriate: (a) under applicable law, including laws outside your state or country of residence; (b) to comply with legal process; (c) to respond to requests from public and government authorities including public and government authorities outside your state or country of residence; (d) to enforce our terms and conditions; (e) to protect our operations or those of any of our affiliates; (f) to protect our rights, privacy, safety or property, and/or that of our affiliates, you or others; and (g) to allow us to pursue available remedies or limit the damages that we may sustain.

## **HOW WE DISCLOSE PERSONAL INFORMATION**

We may disclose Personal Information, including Protected Health Information (defined below) as follows:

- if you are a Patient, to your Provider and/or its Designees and to Authorized Caregivers, without further authorization for purposes of treatment, payment or operations; for

other uses or disclosures permitted by law; or for purposes related to such uses or disclosures.

- if you are an Authorized Caregiver, to the Patient and his/her Provider and/or that Provider's Designees.
- to our third-party service providers who provide services such as website hosting, data analysis, payment processing, order fulfillment, infrastructure provision, IT services, customer service, email delivery services, credit card processing, backup, auditing services and other similar services.
- to a third party in the event of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or capital stock (including in connection with any bankruptcy or similar proceedings).
- as we believe to be necessary or appropriate: (a) under applicable law, including laws outside your state or country of residence; (b) to comply with legal process; (c) to respond to requests from public and government authorities including public and government authorities outside your state or country of residence; (d) to enforce our terms and conditions; (e) to protect our operations or those of any of our affiliates; (f) to protect our rights, privacy, safety or property, and/or that of our affiliates, you or others; and (g) to allow us to pursue available remedies or limit the damages that we may sustain.

## **PROTECTED HEALTH INFORMATION ("PHI")**

"Protected Health Information" or PHI includes information, whether oral or recorded in any form or medium, that we receive from a Patient, his/her Authorized Caregiver, a Provider or that we create on behalf of a Provider, (i) that relates to the past, present or future physical or mental condition of the Patient; the provision of health care to the Patient; or the past, present or future payment for the provision of health care to the Patient; and (ii) that identifies the Patient or with respect to which there is a reasonable basis to believe the information can be used to identify the Patient. "Protected Health Information" has the same meaning generally in this Privacy Policy as defined as the term "Protected Health Information" in 45 C.F.R. § 160.103.

## **HOW WE USE AND / OR DISCLOSE PROTECTED HEALTH INFORMATION**

We may use and/or disclose Protected Health Information in the same manner as Personal Information, as described above, except our use and disclosure of Protected Health Information is further limited as provided by the administrative simplification provision of the Health

Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH”) and the Omnibus regulations promulgating Standards for Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information promulgated thereto.

Specifically, as described above, all uses or disclosures of PHI shall require the Patient’s authorization or a valid authorization on the Patient’s behalf, except: (1) uses or disclosures by or to the Patient; (2) uses or disclosures for consented research, treatment, payment or healthcare operations; (3) as part of any valid use or disclosure; or (4) in compliance with and pursuant to applicable law.

Specific examples of purposes for which the disclosure of PHI by DatStat would require Patient’s valid authorization include: (1) for most uses and disclosures of psychotherapy notes; (2) for use or disclosure of PHI for marketing purposes; (3) for disclosures that constitute a sale of PHI; or (4) for other uses or disclosures that are not exempt from the authorization requirement.

We will enter into business associate agreements with the Patient’s Providers who are “Covered Entities” when we are a “Business Associate,” [as those terms are defined by HIPAA](#). We will use and disclose Protected Health Information only for those uses and disclosures permitted by HIPAA and under the applicable business associate agreement. We may use or disclose Protected Health Information to provide Services to the Patient or his or her Provider. We may also use Protected Health Information for our proper management and administration or to carry out our legal responsibilities.

## **NON-PERSONAL INFORMATION**

“Non-Personal Information” is any information that does not reveal your specific identity, such as any of the following:

- Browser information
- Information collected through cookies, pixel tags and other technologies
- Demographic information and other information provided by you
- Aggregated information

We and our third-party service providers may collect Non-Personal Information in a variety of ways, including:

- Through your browser: Certain information is collected by most browsers, such as your Media Access Control (MAC) address, computer type (Windows or Macintosh), screen resolution, operating system version and Internet browser type and version.
- Using cookies: Cookies allow a web server to transfer data to a computer for recordkeeping and other purposes. We use cookies and other technologies to, among other things, better serve you with more tailored information and facilitate your ongoing access to and use of the Services. We use two types of cookies, “session” cookies and “persistent” cookies. A session cookie is temporary and expires after you end a session and close your web browser. We use session cookies to help customize your experience as you use the Services and maintain your signed-on status as you navigate through the features of the Services. Persistent cookies remain on your hard drive after you have exited from our Services, until you erase them or they expire. If you do not want information collected through the use of cookies, there is a simple procedure in most browsers that allows you to decline the use of cookies. To learn more about cookies, please visit <http://www.allaboutcookies.org/>.
- Using pixel tags, web beacons, clear GIFs or other similar technologies: These may be used in connection with some Site pages and HTML-formatted email messages to, among other things, track the actions of Site users and email recipients, and compile statistics about Site usage and response rates.
- From you: Information such as your location, as well as other information, such as your preferred means of receiving messages through the Services (e.g., emails or text messages), is collected when you voluntarily provide this information. Unless combined with Personal Information, this information does not personally identify you or any other user of the Service.
- By aggregating information: Aggregated Personal Information does not personally identify you or any other user of the Service (for example, we may use Personal Information to calculate the percentage of our users who have chosen to receive messages by text messaging).

## **HOW WE USE AND DISCLOSE NON-PERSONAL INFORMATION**

Because Non-Personal Information does not personally identify you, we may use and disclose Non-Personal Information for any purpose whatsoever. In some instances, we may combine Non-Personal Information with Personal Information (such as combining your name with your geographical location). If we combine any Non-Personal Information with Personal Information, the combined information will be treated by us as Personal Information as long as it is combined.

## **IP ADDRESSES**

Your “IP Address” is a number that is automatically assigned to the computer that you are using by your Internet Service Provider (ISP). An IP Address is identified and logged automatically in our server log files whenever a user uses the Services, along with the time of the visit and the page(s) that were visited. Collecting IP Addresses is standard practice on the Internet and is done automatically by many web sites.

We use IP Addresses for purposes such as calculating usage levels, helping diagnose server problems, and administering the Services. We may also use and disclose IP Addresses for all the purposes for which we use and disclose Personal Information. Please note that we treat IP Addresses, server log files and related information as Non-Personal Information, except where we are required to do otherwise under applicable law.

## **THIRD PARTY SITES**

This Privacy Policy does not address, and we are not responsible for, the privacy, information or other practices of any third parties. The inclusion of a link within the Services does not imply endorsement of the linked site by us or by our affiliates.

## **SECURITY**

We use reasonable organizational, technical and administrative measures to protect Personal Information under our control, consistent with the Department of Health and Human Services Standards for Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information. Unfortunately, no data transmission over the Internet or data storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any account you might have with us has been compromised), please immediately notify us of the problem by contacting us in accordance with the “*Contacting Us*” section below.

Likewise, DatStat will notify affected Providers and Patients of any breach of unsecured PHI within twenty-four (24) hours of notice and confirmation thereof.

## **CHOICE – LIMITING, ACCESSING AND CHANGING YOUR INFORMATION**

If you would like to review, correct, update, delete or otherwise limit our use of your Personal Information that has been previously provided to us, you may contact us in accordance with the “*Contacting Us*” section below.

In your request, please make clear what information you would like to have limited or changed, whether you would like to have your Personal Information deleted from our database or otherwise let us know what limitations you would like to put on our use of your Personal Information. We will try to comply with your request as soon as reasonably practicable.

Please note that in order to comply with certain requests to limit use of your Personal Information we may need to terminate your account with us and your ability to access and use the Services, and you agree that we will not be liable to you for any such termination or for any refunds of prepaid fees paid by you. Although we will use reasonable efforts to do so, you understand that it may not be technologically possible to remove from our systems every record of your Personal Information. The need to back up our systems to protect information from inadvertent loss means a copy of your Personal Information may exist in a non-erasable form that will be difficult or impossible for us to locate or remove.

## **RETENTION PERIOD**

We will retain your Personal Information for the period necessary to fulfill the purposes outlined in this Privacy Policy and our Terms of Service unless a longer retention period is required or allowed by law.

## **USE OF SITE BY MINORS**

The Services are not permitted for use by individuals under the age of eighteen (18) unless they have provided the written consent of their parents or legal guardians, and we request that these individuals do not provide Personal Information to us.

## **UPDATES TO THE PRIVACY POLICY**

We may change this Privacy Policy. The “*Last Updated*” legend at the beginning of this Privacy Policy notes when this Privacy Policy was last revised. Any changes to this Privacy Policy will become effective when we post the revised Privacy Policy on the Site, make it available through

the Services, or otherwise notify you at the email address provided by you at the time you registered for the Services, whichever occurs earlier. Any change to this Privacy Policy will be effective for all information that we maintain, even information in existence before the change. Your use of the Site following these changes means that you accept the revised Privacy Policy.

## **PRIVACY SHIELD**

DatStat complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from European Union and Switzerland to the United States, respectively. DatStat has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit <https://www.privacyshield.gov/>

In compliance with the US-EU and Swiss-US Privacy Shield Principles, DatStat commits to resolve complaints about your privacy and our collection or use of your personal information. European Union or Swiss individuals with inquiries or complaints regarding this privacy policy should first contact DatStat at:

Email: [privacy@datstat.com](mailto:privacy@datstat.com), or please write to: 720 3<sup>rd</sup> Ave, Suite 1000, Seattle, WA 98104. Please note that email communications are not always secure; so please do not include sensitive information in your emails to us.

DatStat has further committed to refer unresolved privacy complaints under the EU-US and Swiss-US Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit <http://www.bbb.org/EU-privacyshield/for-eu-consumers> for more information and to file a complaint.

You may also refer a complaint to your local data protection authority, and we will work with them to resolve your concern. In certain circumstances, the Privacy Shield Framework provides the right to invoke binding arbitration to resolve complaints not resolved by other means, as described in [Annex I to the Privacy Shield Principles](#).

DatStat is subject to the investigatory and enforcement powers of the US Federal Trade Commission (FTC).



In the context of an onward transfer, DatStat has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The DatStat shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

## **CONTACTING US**

If you have any questions about this Privacy Policy, please contact us by email at [privacy@datstat.com](mailto:privacy@datstat.com), or please write to: 720 Third Avenue, Suite 1000, Seattle, WA 98104. Please note that email communications are not always secure; so please do not include sensitive information in your emails to us.