

SSDC Services' Privacy Statement

In compliance with the HIPAA federal and state regulations and to ensure confidentiality, SSDC Services has:

1. Implemented Privacy Policies & Procedures,
2. Developed and implemented required forms,
3. Conducted Staff training regarding HIPAA awareness and updates, and
4. Established safeguards to protect patient health information.

Your privacy is very important to SSDC Services. We maintain high standards regarding the protection of your privacy.

Data Collection

SSDC Services undertakes to collect Your Data by means that are:

- fair;
- legal; and
- transparent.

If you visit SSDC Services' web-site, your web-browser automatically discloses, and SSDC Services' web-server automatically logs, the following information: the date and time, the IP address from which you issued the request, the type of browser and operating system you are using, the URL of any page that referred you to the page, the URL you requested, and whether your request was successful. This data may or may not be sufficient to identify you.

Any additional data that you provide, e.g. in a web-form, may also be logged. This data may or may not be sufficient to identify you.

Any additional data that your web-browser automatically provides may also be logged. This will be the case, for example, if your browser has previously been requested to store data on your computer in '**cookies**' and submits them each time you request a web-page within a particular domain (such as SSDCServices.com or SSDCReports.com). This data may or may not be sufficient to identify you.

If you disclose personal data to SSDC Services in conjunction with an identifier such as your name or your credit-card details, SSDC Services will collect Your Data. Moreover, any data that becomes available to SSDC Services through any of the means described in the preceding paragraphs may be able to be associated with that identifier, and hence become Your Data.

Subject to the qualifications immediately below, SSDC Services undertakes to collect Your Data **from you** and not from other parties. This undertaking is qualified as follows:

- Where SSDC Services reasonably considers that the protection of its financial interests requires that it gather Your Data from other sources, or from additional sources. This applies in particular where SSDC Services has a lending exposure to you, and seeks information about your creditworthiness;
- Where SSDC Services reasonably considers that its capability to deliver quality services to you will be materially enhanced by gathering Your Data from other sources. This applies in particular to consumer profile data.

Where SSDC Services collects Your Data from sources other than you, it undertakes:

- to do so only by legal means;
- to do so only with your Consent; and
- to declare to you what sources it uses, and under what circumstances.

SSDC Services undertakes to declare the **purpose of collection** in a manner which is clear and meaningful, and to avoid vague, highly inclusive statements such as 'to support our operations'.

Data Security

SSDC Services undertakes to **store** Your Data in a manner that ensures security against unauthorized access, alteration or deletion, at a level commensurate with its sensitivity.

SSDC Services undertakes to store Your Data only in **jurisdictions** where data protections are at least equivalent to those required under the OECD Guidelines.

SSDC Services undertakes to **transmit** Your Data in a manner that ensures security against unauthorized access, alteration or deletion, at a level commensurate with its sensitivity.

SSDC Services undertakes to implement appropriate **measures to ensure security of Your Data against inappropriate behavior by SSDC Services' staff-members and contractors**. These include:

- training for staff in relation to privacy;
- access control, to limit access to Your Data to those staff and contractors who have legitimate reasons to access it;
- particularly in the case of sensitive data, audit trails of accesses, including the identities of staff and contractors accessing the data;
- reminders to staff and contractors from time to time about the importance of data privacy, and the consequences of inappropriate behavior;
- declaration of appropriately strong sanctions that are to be applied in the event of inappropriate behavior
- clear communication of policies and sanctions; and
- processes to audit, to investigate and to impose sanctions.

Data Use

Use refers to the application of Your Data by any part of SSDC Services, or any staff-member or contractor of SSDC Services in the course of their work.

SSDC Services undertakes to use Your Data only for:

- **the purposes for which it was collected;**
- such other purposes as are **subsequently agreed** between SSDC Services and You;
- such additional purposes as may be **required by law**. In these circumstances, SSDC Services will take any reasonable steps available to it to communicate to You that the use has occurred, unless it is precluded from doing so by law; and
- such additional purposes as are **authorized by law** (in particular to protect SSDC Services' interests, e.g. if it believes on reasonable grounds that You have failed to fulfil your undertakings to SSDC Services or have committed a breach of the criminal law).

SSDC Services undertakes to use Your Data only if it has **demonstrable relevance** to the particular use to which it is being put.

SSDC Services undertakes to use Your Data in such a manner as to take into account the possibility that it is not of **sufficient quality for the purpose**, e.g. because it is inaccurate, out-of-date, incomplete, or out-of-context.

Data Disclosure

Disclosure refers to making Your Data available to any party other than SSDC Services and You. The term disclosure may include many different conditions of data transfer, including selling, renting, trading, sharing and giving.

SSDC Services undertakes to disclose Your Data only under the following circumstances:

- **in the course of business being conducted between You and SSDC Services**, where disclosure is necessary to a contractor, such as a transport company. Where Your Data is disclosed in this way, SSDC Services undertakes to exercise control over SSDC Services' contractors to ensure that their actions are compliant with these Terms;
- **in other circumstances that are directly implied by the purpose agreed between You and SSDC Services** at the time of data collection or subsequently. Where Your Data is disclosed in this way, SSDC Services undertakes to exercise control over SSDC Services' contractors to ensure that their actions are compliant with these Terms;
- **with your consent**, or at your request;
- **where required by law**, such as a provision of a statute, or a court order such as a search warrant or Subpoena. In these circumstances, SSDC Services will take any reasonable

steps available to it to communicate to You that the disclosure has occurred, unless it is precluded from doing so by law;

- **where permitted by law** (e.g. the reporting of suspected breach of the criminal law to a law enforcement agency; and in an emergency, where SSDC Services believes on reasonable grounds that the disclosure of Your Data will materially assist in the protection of the life or health of some person), provided that SSDC Services will apply due diligence to ensure that the exercise of the permission is justifiable.

In all cases, SSDC Services undertakes to disclose only such of Your Data as is necessary in the particular circumstances.

Data Retention and Destruction

Subject to the qualifications immediately below, SSDC Services undertakes:

- to **retain** Your Data only as long as is consistent with its purpose or when applicable law permits for most data this will be within 90 Days; and
- to **destroy** Your Data when its purpose has expired, and to do so in such a manner that Your Data is not subsequently capable of being recovered.

This undertaking is qualified as follows:

- Your Data may be retained in SSDC Services' **logs, backups and audit trails** within short-term retention cycles that are devised to protect the company's operations. In such cases, Your Data will be destroyed in accordance with those cycles. SSDC will hold all logs for a period of 3 years in accordance with the HIPAA requirements;
- Your Data may be retained beyond the expiry of its purpose if that is **required by law**, such as a provision of a statute, or a court order such as a search warrant or Subpoena, or a warning by a law enforcement agency that delivery of a court order is imminent. In these circumstances, SSDC Services:
 - will take any reasonable steps available to it to communicate to You that Your Data is being retained, unless it is precluded from doing so by law; and
 - will only retain Your Data while that provision is current, and will then destroy Your Data;
- Your Data may be retained beyond the expiry of its purpose if it is **authorized by law** (in particular to protect SSDC Services' interests, e.g. if it believes on reasonable grounds that You have failed to fulfil your undertakings to SSDC Services or have committed a breach of the criminal law). In these circumstances, SSDC Services will only retain Your Data while that situation is current, and will then destroy Your Data.

Access by You to Your Personal Data

SSDC Services undertakes to provide you with **access** to Your Data, subject to only such conditions and processes as are reasonable in the circumstances. In particular, SSDC Services undertakes to enable access:

- conveniently;
- without unreasonable delay;
- In an understandable format and
- without cost.

SSDC Services undertakes to establish and operate **identity authentication protections for access to Your Data** that are appropriate to its sensitivity, but practical. This may involve some inconvenience; for example, relatively straightforward procedures may be involved in order to provide you with access through a channel that you have previously registered with SSDC Services (such as a particular email-address), but may impose more onerous procedures if you wish to use some other channel.

In the event that you dispute some aspect of Your Data, SSDC Services undertakes to take reasonable steps in relation to the **amendment, supplementation or deletion** of Your Data.

You undertake:

- not to seek access for frivolous purposes, or unreasonably frequently;
- to accept that deletion of some data may not be consistent with the provision of particular services by SSDC Services to you.

Information about Data-Handling Practices

SSDC Services undertakes to make information available to you about the manner in which SSDC Services handles your data:

- in general terms, in a readily accessible manner; and
- in more specific terms, on request.

Where Your Data is disclosed to a contractor, SSDC Services undertakes to make information available to you on request about the manner in which SSDC Services' contractors handle your data.

SSDC Services undertakes to ensure that the information provided is meaningful, and addresses your concerns.

You undertake:

- not to seek such information for frivolous purposes, or unreasonably frequently; and
 - to accept that the disclosure of excessive detail may harm the security of Your Data and SSDC Services' business processes, and may harm SSDC Services' commercial interests.
-

Handling of Enquiries, General Concerns and Complaints

If you have enquiries, general concerns, or complaints about these Terms, or about SSDC Services' behavior in relation to these Terms, you undertake:

- to **communicate them in the first instance:**
 - to SSDC Services only;
 - in sufficient detail;
 - through a channel made available by SSDC Services for that purpose;

SSDC Services undertakes:

- to provide one or more **channels for communications** to SSDC Services, which are convenient to users;
- to promptly provide **acknowledgement** of the receipt of communications, including the provision of a copy of the communication, the date and time it was registered, and SSDC Services' reference-code for the communication;
- to promptly provide **a response** to the communication, in an appropriate and meaningful manner.

You further undertake to not pursue SSDC Services through any **Regulator or the media:**

- until and unless SSDC Services has had a reasonable opportunity to respond to the initial communication; and
 - while SSDC Services and you are conducting a meaningful dialogue about the matter.
-

Enforcement

SSDC Services declares that its undertakings in these Terms are intended to create **legal obligations**, and that those obligations are intended to be **enforceable** under appropriate laws in appropriate jurisdictions. These include laws relating to data protection, privacy, fair trading, corporations and criminal laws.

You undertake to seek enforcement only in a **jurisdiction** that is relevant to the transactions that have taken place between You and SSDC Services, in particular the jurisdiction in which you

live or in which you performed the relevant acts, and the jurisdiction in which SSDC Services is domiciled or performed the relevant acts.

Changes to These Privacy Undertakings

SSDC Services undertakes:

- not to unilaterally make any material change to these Terms in a manner that reduces the protections for Your Data;
 - to take all practicable steps to prevent any company that acquires this company or any of its relevant assets from materially changing the Terms applicable to Your Data in a manner that reduces the protections for Your Data;
 - where it is considering making changes to these Terms, or creating more specific Terms relating to specific services, to consult with appropriate representative and advocacy organizations;
 - where it makes changes to these Terms, to ensure that the differences between successive versions are readily accessible;
 - to maintain all prior versions of these Terms in such a manner that they are dated, and readily accessible.
-

Privacy Officer Assignment

Bonnie Donahue has been assigned Privacy Officer. As the assigned privacy officer her responsibilities are as follows.

- a. Understanding the HIPAA Privacy Rule and how it applies within each Covered Component.
- b. Developing appropriate policies and procedures to comply with the HIPAA Privacy Rule.
- c. Overseeing the enforcement of patient privacy rights within each Covered Component.
- d. Monitoring each Covered Component for compliance with privacy policies and procedures.
- e. Developing and implementing privacy training for employees within each Covered Component.
- f. Notifying the Security Officer of any Business Associate Agreements that implicate EPHI, prior to the execution or amendment of any such agreement.
- g. Receiving and responding to complaints of alleged non-compliance with the HIPAA Privacy Rule.
- h. Oversees and ensures the right of the practice/organization's patients to inspect, amend and restrict access to protected health information, when appropriate.
- i. Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the practice/organization's privacy

policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.

- j. Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the entities other compliance and operational assessment functions.
 - k. Works with legal counsel and management, key departments, and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.
 - l. Initiates, facilitates and promotes activities to foster information privacy awareness within the organization and related entities.
 - m. Maintains current knowledge of applicable federal and state privacy laws and accreditation standards, and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.
-

Definitions

SSDC Services means SSDC Services Corp.

Your Data means data that is capable of being associated with you, whether or not it includes an explicit identifier such as your name or customer number. In particular, it encompasses all data that SSDC Services is capable of correlating with you, using such means as server-logs and cookie-contents.

Your Data does not refer to data that can no longer be associated with you. This includes aggregated data that does not and cannot identify the individuals whose data are included in the aggregation.

Consent means your concurrence with an action to be taken by SSDC Services. Consent may be express or implicit, but in either case must be informed and freely-given.