Data Protection and Security Policies - HIPAA and GDPR

Date of Publication: October 2nd, 2018

Rationale

iProcedures is committed to a policy of protecting the rights and privacy of individuals, including staff and others, in accordance with HIPAA and General Data Protection Regulation (GDPR).
The new regulatory environment demands higher transparency and accountability in how applications manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that the applications will need to be aware of as data controllers, including provisions intended to enhance the protection of patient's personal data.
To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) iProcedures must ensure that all the information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance
This policy applies to all staff of iProcedures. Any breach of this policy or of the Regulation itself will be considered an offence and disciplinary procedures will be invoked. This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to HIPAA, GDPR and other relevant legislation.

Data Protection and Security Policy

1. **About this Policy**

The types of Personal Data that iProcedures LLC, a company incorporated in Florida ("**iProcedures**", "**we**", "**us**", "**our**") may be required to handle include information about current, past and prospective clients, customers, contractors, and any other users of any of our services and others that we communicate with for the purposes of carrying out our business. The Personal Data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards including those specified in the General Data Protection Regulation, Regulation (HIPAA) and other regulations (GDPR).

This policy and any other documents referred to in it sets out the basis on which we will process any Personal Data we collect from Data Subjects, or that is provided to us by Data Subjects or other sources. Data Users are obliged to comply with this policy when Processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action. This policy focuses on our obligations as a Data Controller and we may be under different or additional obligations in respect of any Processing which we carry out as a Data Processor.

This Policy will be reviewed at least once a year and periodically updated by the Data Protection Officer to reflect any changes in legislation or in our methods or practices.

2. **Definitions**

2.1 **Data Subjects** means all living identifiable individuals about whom we hold Personal Data. All Data Subjects have legal rights in relation to their personal information.

2.2 **Personal Data** means data relating to a living individual who can be identified, directly or indirectly, from that data (or from that data and other information in our possession). Personal Data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behavior.

2.3 **Data Controllers** are the people who, or organizations which, determine the purposes for which, and the manner in which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the current regulations. **Data Users** are those of our employees and contractors whose work involves Processing Personal Data. Data Users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

2.4 **Data Processors** include any person or organization that processes Personal Data on our behalf and on our instructions.

2.5 **Website** means our website at https://www.iProcedures.com/.

2.6 **Processing** is any activity or set of activities which is performed on Personal Data or sets of Personal Data, whether or not by automated means. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organizing, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.

2.7 **Profiling** means any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, locations or movements.

2.8 **Sensitive Personal Data** includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, physical or mental health or condition or sexual life. Sensitive Personal Data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

2.9 **Services** means: access to the relevant iProcedures applications provided via Customer's unique URL

3. Accountability

The accountability principle requires organizations to be able to demonstrate compliance with data protection requirements. We need to ensure data protection compliance is integrated into any new technology planning or new Processing activities.

The Data Protection Officer is responsible for ensuring compliance with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer.

All iProcedures employees have a responsibility to comply with this policy and are required to complete appropriate training to ensure compliance with this policy.

4. Data Protection Principles

Anyone Processing Personal Data must comply with principles of good practice. These provide that Personal Data must be:

- Processed fairly, lawfully and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.
- Accurate and where necessary, kept up to date. Where Personal Data is inaccurate with regards to the purpose for which it is processed, every reasonable step must be taken to either erase or rectified it without delay.
- Not kept longer than necessary for the purpose for which the Personal Data is processed.
- Processed in line with Data Subjects' rights.
- Processed in a manner that ensures appropriate security of the Data Subject, including protection against unauthorized Processing and accidental loss, destruction or damage.
- Not transferred to people or organizations situated in countries without adequate protection without putting in place appropriate safeguards.

5. Processing for Limited Purposes

In the course of our business, we may collect and Process Personal Data. This may include data we receive directly from a Data Subject (for example, by completing forms) and data we receive from other sources (including, for third party vendors).

We will only Process Personal Data for the specific purposes set out in our Privacy Policy or for any other purposes specifically permitted by the regulations.

6. Categories of Data Subjects

iProcedures collects and processes a range of information. This includes:

- Name, address and contact details, including email address and telephone number, date of birth and gender;
- Information about your marital status, next of kin, dependents and emergency contacts;
- Information about medical or health conditions, labs, diagnostic studies.

7. Data protection impact assessment

In the event new Processing activities are introduced or we develop new technologies into our business, an assessment of the impact of the change in operations on the protection of such Personal Data shall be carried out in order to address any Processing operations that present a high risk to the rights and freedoms of the Data Subjects or risk non-compliance with the regulations.

8. Data Security

The following policy describes how iProcedures handles personal data within the organization and the key data privacy principles which it complies with.

iProcedures takes the security of your data seriously. iProcedures has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where iProcedures engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Company measures to ensure the security of data.

We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- **Confidentiality** means that only people who are authorized to use the data can access it.
- **Availability** means that authorized users should be able to access the data if they need it for authorized purposes.

Security procedures include:

- **Physical security controls.** iProcedures facilities feature controls (e.g., access control badges) to prevent unauthorized access.
- **Methods of disposal.** Paper documents are shredded, and digital storage media are physically destroyed or securely overwritten when they are no longer required.
- **Equipment.** Data Users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC or lock the session when it is left unattended.

- **Incident Management.** iProcedures maintains security incident management policies and procedures. iProcedures notifies impacted Data Subjects without undue delay of any unauthorized disclosure of their respective Personal Data by iProcedures or its agents of which iProcedures becomes aware to the extent required by Data Protection Laws and Regulations.
- **Technical safeguards.** iProcedures ensures that technical and organizational measures are in place to ensure data security and minimization, this includes anti-virus, intrusion detection, user authentication services, and encryption of data where appropriate.

9. Reporting Breaches

Where there has been a Personal Data breach and the breach is likely to result in a high risk to the rights and freedoms of the Data Subject, we will report the breach to the concerned parties without undue delay and, where feasible, not later than 72 hours after having become aware of it.

Data Processor Security Controls

1. Nature and Purpose of Processing

iProcedures will Process Personal Data as necessary to perform the iProcedures services and as further instructed by the Customer in its use of the Services.

2. Data Segregation

The Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data storage and access based on business needs. The architecture provides an effective logical data separation for different Customers via Customer-specific unique IDs and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

3. Security Controls

iProcedures has implemented procedures designed to ensure that Customer Data is processed only as instructed by the Customer, throughout the entire chain of processing activities by iProcedures. Additionally, the Services undergo security assessments by internal personnel and third parties, which include application security assessments.

iProcedures adopts a number of security controls, which include:

- Controls to ensure initial passwords must be reset on first use;
- Password length and complexity requirements;
- Customers have the option to integrate Single Sign-On technologies to directly control the authentication and credential complexity, expiration, account lockout, IP white/black listing etc.;
- Customers have the option to manage their application users, define roles, and apply permissions and rights within their implementation of the Services;
- User passwords are stored using a salted hash format and are not transmitted unencrypted;

- User access log entries will be maintained, containing date, time, User ID, URL executed, or identity ID operated on, operation performed (accessed, created, edited, deleted, etc.);

- If there is suspicion of inappropriate access to the Services, iProcedures can provide Customer log entry records to assist in analysis. This service will be provided to Customers on a time and materials basis;

- User access logs will be stored in a secure centralized host to prevent tampering;

4. Intrusion Detection

iProcedures, or an authorized independent third party, will monitor the Services for unauthorized intrusions using network-based intrusion detection mechanisms.

5. Security Logs

All iProcedures systems used in the provision of the Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to facilitate security reviews and analysis.

6. Incident Management

iProcedures maintains security incident management policies and procedures. iProcedures notifies impacted Customers without undue delay of any unauthorized disclosure of their respective Customer Data by iProcedures or its agents of which iProcedures becomes aware to the extent required by Data Protection Laws and Regulations.

7. User Authentication

Access to the Services requires a valid user ID and password combination (or via integrated Single Sign-On mechanism), which are encrypted via TLS while in transmission.

8. Physical Security

Production data centers used to provide the Services have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other predictable natural conditions, are secured by around the-clock guards, two-factor access screening,

including biometrics, and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

9. Personnel Security

iProcedures employment offers are contingent upon successful completion of criminal background and reference checks. Upon commencing employment, all iProcedures employees receive information security training and are contractually committed to confidentiality clauses to ensure that they adhere to iProcedures's commitment to security and confidentiality for its customers. iProcedures's information security awareness and training program requires employees complete annual security refresher training.

10. Reliability and Backup

All infrastructure components are configured in a high availability mode or in a redundant fashion. All Customer Data submitted to the Services is stored on a redundant fault-tolerant infrastructure that is replicated to the secondary data center hourly. Data centers forming a regional pair are geographically located in different areas to minimize the possibility of a pandemic or natural disaster impacting both at the same time.

11. Disaster Recovery

The Services' production systems are protected by disaster recovery plans which provide for backup of critical data and services. A comprehensive system of recovery processes exists to bring business-critical systems back online within the briefest possible period of time. Recovery processes for database security, systems administration, and network configuration and data provide a roadmap for personnel to make processes available after an outage. The Services' disaster recovery plans currently have at least the following standard target recovery objectives: (a) restoration of the Services (RTO) within 1-3 hours after iProcedures's declaration of a disaster; and (b) maximum Customer Data loss (RPO) of 1-2 hours; excluding, however, a disaster or multiple disasters causing the compromise of multiple data centers at the same time, and excluding development and test bed environments, such as the sandbox service.

12. Viruses

The Services have controls in place that are designed to prevent and detect the introduction of viruses to the Services' respective platforms.

13. Data Encryption

The Services use, or enable Customers to use, industry-accepted encryption products to protect Customer Data and communications during transmissions between a Customer's network and the Services, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum. Any data that is collected and persisted by ONE is encrypted at rest using 256-bit AES encryption. Encryption keys and secrets are safeguarded in a secure data vault that is restricted to authorized users and applications as defined in our access control policy.

14. Change Management

iProcedures's Change Management processes are aligned to ITIL to ensure standardized methods and procedures are used to maximize value while minimizing risk of incidents and disruptions when making changes to the Services. The Change Advisory Board reviews all changes for business and security impacts prior to authorizing a change.

All production systems are provisioned with secure configurations derived from industry best practices and are managed in accordance with iProcedures's asset management and information classification controls.