# DATA PROTECTION POLICY



## CONTENTS


1. DOCUMENT HISTORY 2
2. CLASSIFICATION 2
3. PURPOSE 2
4. SCOPE OF APPLICATION 2
5. RESPONSIBILITIES 2
6. RELATED DOCUMENTATION 2
7. TERMS, ABBREVIATIONS AND DEFINITIONS 3
8. PROCESS DESCRIPTION 4

## 1. DOCUMENT HISTORY

| Revision | Date of enactment | Change author | Change description |
|---|---|---|---|
| *1.0* | *2023-09-11* | | *The document is created.* |

## 2. CLASSIFICATION

Confidential serious.

## 3. PURPOSE

This policy sets out the guidelines for data protection within the company.

## 4. SCOPE OF APPLICATION

This procedure is applicable for all employees and sets out rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal and other sensitive company's information.

The Data Protection Officer is responsible for ensuring compliance with the General Data Protection Regulation (Regulation (EU) 2016/679) and with the procedure.

## 5. RESPONSIBILITIES

**Data Owner – DPO.**

All employees shall be trained according to and comply with the policy.

DPO and QSR responsible for the training of this policy for employees.

In case of not complying with the policy, employee shall write explanatory act to explain the situation. Recurrent noncompliance might lead to dismissal of the employee.

## 6. RELATED DOCUMENTATION

| No. | Title |
|---|---|
| ***Regulatory / normative documents*** | |
| *Applicable regulatory documents related to medical devices and information security are indicated in RG-25.* | |
| ***Internal documents*** | |
| *PS-10* | *Trainings and Competences* |
| *PS-27* | *Security Breach Management (FDA)* |
| *PS-28* | *Reporting to Regulatory Authorities* |
| | *Vidinė analizė skirti Duomenų saugos pareigūną* |
| | *ĮSAKYMAS dėl Duomenų saugos pareigūno paskyrimo* |
| | *ĮSAKYMAS dėl asmens duomenų saugos valdymo atsakomybių delegavimo* |
| | ĮSAKYMAS dėl techninių ir organizacinių asmens duomenų saugumo priemonių patvirtinimo |

| No. | Title |
|---|---|
| | *TECHNINĖS IR ORGANIZACINĖS asmens duomenų saugumo priemonės* |
| | *Asmens duomenų tvarkymo registras* |
| | *Duomenų VALDYTOJO duomenų tvarkymo veiklos įrašai* |
| | *Duomenų TVARKYTOJO duomenų tvarkymo veiklos įrašai* |
| | *Poveikio duomenų apsaugai vertinimo POREIKIS: PRIEŽASTYS IR SPRENDIMAS* |
| | *ĮSAKYMAS dėl Poveikio duomenų apsaugai vertinimo METODOLOGIJOS ir įrašų FORMOS tvirtinimo* |
| | *Poveikio duomenų apsaugai vertinimo įrašai* |
| *RG-5* | *Registry of data security events* |

## 7. TERMS, ABBREVIATIONS AND DEFINITIONS

| Terms/ abbreviations | Definitions |
|---|---|
| ***Data*** | *is information, which is stored electronically, on a computer, or in certain paper-based filing systems.* |
| ***Data subjects*** | *for the purpose of this policy include all living individuals about whom we hold personal data. All data subjects have legal rights in relation to their personal data.* |
| ***Personal data*** | *means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).* |
| ***Data controllers*** | *are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.* |
| ***Data users*** | *include all staff of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (Staff). whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.* |
| ***Data processors*** | *include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition, but it could include suppliers which handle personal data on our behalf.* |
| ***Processing*** | *is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.* |
| ***Sensitive personal data*** | *includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.* |
| ***Supervisory authority*** | *Authority responsible for controlling personal data breaches in particular area.* |
| ***Member state*** | *Country that belongs to EU.* |
| ***Secretary*** | *the Secretary of Health and Human Services and any other officer or employee of the Department of Health and Human Services to whom authority has been delegated.* |

| Terms/ abbreviations | Definitions |
|---|---|
| **Business associate** | *Business associate means, with respect to a covered entity, a person who:*<br>▪ On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing or<br>▪ Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. |
| **Data aggregation** | *Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.* |
| **General Administrative Requirements** | *As described in Code of Federal Regulations Title 45 Subtitle A Subchapter C Part 160.* |
| **Covered entity** | *A health care provider who transmits any health information in electronic form in connection with a transaction.* |

## 8. PROCESS DESCRIPTION

### *8.1.* General information

The data we store, and process includes but is not limited to:

- Confidential – most important data:
  - Personal data:
    - Personal data related to our staff.
    - Customer contact, billing and other customer relationship information.
    - Data contained within our software.
  - Company's secrets
  - Marketing plans
- Internal - sensitive information related to the company:
  - Part of internal procedures, work instructions

- Public information:
  - Brochure
  - Label

**8.2. Training Staff**

All staff members shall undergo basic information security awareness training (PS-10), which includes:

- The Data Protection Principles.
- Information Classification & Handling Procedure.
- Incident Reporting Procedure.

**8.3. Data Protection Principles**

Data must be protected according to the classification levels:

- Public – as information does not need to be protected, no protection rules need to be implemented.
- Internal – data that requires protection rules implemented such as limited access.
- Confidential – data that requires most protection and the strictest rules shall be implemented such as access control, password protection, encryption.

**8.4. Personal Data/Confidential Management**

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- Processed fairly and lawfully.
- Processed for limited purposes and in an appropriate way.
- Adequate, relevant and not excessive for the purpose.
- Accurate.
- Not kept longer than necessary for the purpose.
- Processed in line with data subjects' rights.
- Secure.
- Not transferred to people or organisations situated in countries without adequate protection.

In order to comply with GDPR requirements, internal analysis for the necessity of responsible Data Protection Officer should be carried out. If during analysis, it is decided that there is a need of DPO. He/she is assigned by CEO's order. DPO should be incorporated in all GDPR related matters in a timely manner. DPO has the right to ask for the resources needed for execution of his role including required training. DPO has the obligation to:

- inform data controller or processor and data processing employees about their obligations regarding GDP Regulation and to other Union or Member State data protection provisions.
- monitor compliance with GDP Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.
- provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to GDPR Article 35;
- cooperate with the supervisory authority;
- act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in GDPR Article 36, and to consult, where appropriate, with regard to any other matter.

The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Before handling personal data such as photograph or telephone number, it is necessary to receive signed consent from the data subject. Consent could be added to the contract or as a separate document.

Data subject might ask to provide, correct, delete or restrict processing the information that is handled by the company. In this case as soon as possible but not later than in one month, data controller shall provide handled information, correct, delete it or restrict processing. If data needs to be provided to data subject, it is sent in .pdf or another format that is easy to read by the computer. After request completion, data controller shall send an email to inform about request completion.

Personal data shall not be provided to third parties unless agreed differently. Consent shall be given by data subject in contract or separate document. If data is transferred to a third party at any point, this party is managed as data recipient. Data controller shall inform data recipient, if any data were corrected, deleted or limitation of processing implemented unless it is impossible to do so or would require disproportionate effort. Upon the data subject's request, the data controller shall inform the data subject of those data recipients who received his/her personal data. The communication between these 3 parties could be carried out by emails sending requests or requested information.

Personal data required to execute job rights and duties mentioned in employment contract and/or labour legislation is not classified as personal data covered by GDPR.

In RG-14 is presented the folders with employees who have access to the information.

If necessary, data controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

#### 8.4.1. Fair & Lawful Processing

The intention is not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is.

For personal data to be processed lawfully, certain conditions must be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

#### 8.4.2. Processing for Limited Purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

#### 8.4.3. Adequate, Relevant and Non-excessive Processing

The internal data could be shared within the company in order to provide the most complete service for our customers. Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any personal data which is not necessary for that purpose should not be collected in the first place.

Cooperation with supervisory authority shall be maintained, if there is a request from the authority.

At any point, data subject can use the right to erasure ("right to be forgotten"). In this case, data controller without undue delay has the obligation to erase personal data.

Data subject can restrict data processing for data controller, if:

- data is not accurate,
- processing of personal data is not rightful, but data subject does not agree for data erasure,
- data controller does not need personal data anymore,
- data subject contradicts data processing in accordance with Article 21, paragraph 1 of the Regulation, if the legitimate reasons of the data controller do not outweigh data subject's reasons.

A formal request from a data subject for information that we hold about them must be made in writing. Any member of staff who receives a written request should forward it to their line manager immediately.

In case of a request from a data subject, company should prepare a report/list of personal data in pdf format and provide to the data subject not later than in 5 working days.

#### 8.4.4. Accurate Data

Personal data must be accurate and kept up to date. Information which is incorrect, or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

At any time, data subject can ask to update his data.

#### 8.4.5. Timely Processing

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

#### 8.4.6. Processing in Line with Data Subject's Rights

Personal data must be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

#### 8.4.7. Data Security

We must ensure that appropriate security measures are taken against unlawful or unauthorized processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on company's server.

All employees and relevant interested parties shall comply at all times with the following safety rules:

- Do not let to follow you into office premisses/rooms anyone who does not have access to enter there. Any stranger seen in entry-controlled areas should be reported.
- Do not leave opened doors.
- Keep sensitive documents and information secure and locked away when not in use.
- Lock your computer screen or log out when stepping away from your desk.
- Report all security events to the company's Data Protection Officer by email: a.kiziela@ligence.io
  Employees can also report observed security events anonymously by filling out the e. form at: https://www.ligence.io/anonymous-security-event-report.
- If employee receives a suspicious email requesting personal data, do not open any attachments and delete the email. If you start receiving this type of email on a regular basis, please inform ISO.
- Confidential data which is sent by email must be protected with a ZIP password.

- When sending personal data and other documents, make sure that only the persons to whom the information is addressed receive and have access to it. For example, software codes and other confidential information should not be sent.
- All data relating to company information, whether confidential, internal or public, must be stored in company repositories, but NOT in personal repositories (dropbox, personal google drive, etc.).
- Paper documents (confidential, internal) should be forwarded to Project manager for destruction.
- Employees are prohibited from installing and using unlicensed, illegal software on devices belonging to UAB Ligence.
- Due to the increased risk of data leakage, illegal content and viruses, employees are strictly forbidden to install and use P2P, Torrent, other similar applications.
- Do not disclose any login details to anyone when talking on the phone.
- Never click on links if you receive emails, social networking messages, text messages or other messages and links asking you to enter and change your passwords (unless you have initiated this yourself).
- Always keep your operating system up-to-date.
- Always keep your antivirus and firewall programs running.
- Always use a VPN when connecting to company data, drives and other network storage.
- Access to company data and networks from public computers is prohibited.
- In case of security and privacy events employees are not allowed to:
    - Conceal/ignore evidence.
    - Share security event information with others or with Ligence employees who do not need the information.
    - Try to investigate or mitigate the security event themselves.

**8.4.8. Providing Information over the Telephone**

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. They should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

Refer to their line manager or the Data Protection Officer (DPO) for assistance in difficult situations. No-one should be bullied into disclosing personal information.

**8.5. Data breach incidents**

Data breach incidents including personal data breach incidents are reported according to PS-28.

**8.6. Access Restriction**

Access restriction requirements:

- Not allowing access to sensitive information by unknown user identities or anonymously. Public or anonymous access should only be granted to storage locations that do not contain any sensitive information.
- Providing configuration mechanisms to control access to information in systems, application and services.
- Controlling which data can be accessed by a particular user.
- Controlling which identities or group of identities have which access, such as read, write, delete and execute.
- Providing physical or logical access controls for the isolation of sensitive applications, application data or systems.
- Dynamic access management techniques and processes to protect sensitive information that has high value to the organization should be considered when the organization:
- Needs granular control over who can access such information during what period and in what way.

- Wants to share such information with people outside the organization and maintain control over who can access it.
- Wants to dynamically manage, in real-time, the use and distribution of such information.
- Wants to protect such information against unauthorized changes, copying and distribution (including printing).
- Wants to monitor the use of the information.
- Wants to record any changes to such information that take place in case a future investigation is required.
- Dynamic access management techniques should protect information throughout its life cycle (i.e., creation, processing, storage, transmission and disposal), including:
    - Establishing rules on the management of dynamic access based on specific use cases considering: granting access permissions based on identity, device, location or application; leveraging the classification scheme in order to determine what information needs to be protected with dynamic access management techniques.
    - Establishing operational, monitoring and report process and supporting technical infrastructure.
- Dynamic access management systems should protect information by:
    - Requiring authentication, appropriate credentials or a certificate to access information
    - Restricting access, for example to a specified time frame.
    - Using encryption to protect information.
    - Defining the printing permissions for the information.
    - Recording who access the information and how the information is used.
    - Raising alerts if attempts to misuse the information are detected.

### 8.7. Privacy management of individual Identifiable Health Information in US

#### 8.7.1. Uses and disclosures of protected health information: General rules

Covered entity or business associate (UAB "Ligence") may not use or disclose protected health information, except as permitted or required by this subpart or General Administrative Requirements.

***Business associates: Permitted uses and disclosures.***

UAB "Ligence" may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to Business associate contracts or as required by law. UAB "Ligence" may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes:

- The contract may permit UAB "Ligence" to use and disclose protected health information for the proper management and administration of UAB "Ligence", as provided in paragraph Other requirements for contracts and other arrangements of this section; and
- The contract may permit UAB "Ligence" to provide data aggregation services relating to the health care operations of the covered entity.

If such uses or disclosures are permitted by its contract or other arrangement.

***Business associates: Required uses and disclosures.***

A business associate is required to disclose protected health information:

When required by the Secretary under General Administrative Requirements to investigate or determine the business associate's compliance with this subchapter.

To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations:

- Notwithstanding that the covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual, if the protected health information that is the subject of a request for access is

maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

- If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

with respect to an individual's request for an electronic copy of protected health information.

***Prohibited uses and disclosures.***

*Sale of protected health information:*

Except pursuant to and in compliance with Authorization required: Sale of protected health information. covered entity or UAB "Ligence" may not sell protected health information.

Sale of protected health information does not include a disclosure of protected health information: a disclosure of protected health information by covered entity or UAB "Ligence", if applicable, where covered entity or UAB "Ligence" directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.

Sale of protected health information does not include a disclosure of protected health information:

- For public health purposes pursuant to Uses and disclosures for public health activities or Limited data set.
- For research purposes pursuant to Uses and disclosures for research purposes or Limited data set, where the only remuneration received by covered entity or UAB "Ligence" is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;
- To or by a UAB "Ligence" for activities that the UAB "Ligence" undertakes on behalf of covered entity, or on behalf of a UAB "Ligence" in the case of a subcontractor, pursuant to Disclosures to UAB "Ligence"s and UAB "Ligence" contracts and the only remuneration provided is by covered entity to the UAB "Ligence", or by the UAB "Ligence" to the subcontractor, if applicable, for the performance of such activities;
- To an individual, when requested under Access of individuals to protected health information or Accounting of disclosures of protected health information;
- Required by law as permitted under Uses and disclosures required by law; and
- For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by covered entity or UAB "Ligence" is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

*Minimum necessary* - When using or disclosing protected health information or when requesting protected health information from another covered entity or UAB "Ligence", covered entity or UAB "Ligence" must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

*Minimum necessary does not apply.* This requirement does not apply to:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to the individual, as permitted to the individual; or To an individual, when requested under, and required by Access of individuals to protected health information or Accounting of disclosures of protected health information; and;
- Uses or disclosures made pursuant to an authorization under Uses and disclosures for which an authorization is required;
- Disclosures made to the Secretary;
- Uses or disclosures that are required by law.

***Uses and disclosures to create de-identified information.***

A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a UAB "Ligence" for such purpose, whether or not the de- identified information is to be used by covered entity.

***Uses and disclosures of de-identified information.***

Health information that meets the standard and implementation specifications for de-identification under De-identification of protected health information and Requirements for de-identification of protected health information is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this part do not apply to information that has been de-identified in accordance with the applicable requirements of Other requirements relating to uses and disclosures of protected health information, provided that:

- Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and
- If de-identified information is re-identified, a covered entity may use or disclose such re- identified information only as permitted or required by this part.

***Disclosures to business associates***

A covered entity may disclose protected health information to a UAB "Ligence" and may allow a UAB "Ligence" to create, receive, maintain, or transmit protected health information on its behalf, if covered entity obtains satisfactory assurance that the UAB "Ligence" will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a UAB "Ligence" subcontractor.

A UAB "Ligence" may disclose protected health information to the other business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the UAB "Ligence" obtains satisfactory assurances, in accordance with UAB "Ligence" contracts, that the subcontractor will appropriately safeguard the information.

***Documentation.*** The satisfactory assurances required by Disclosures to business associates must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of business associate contracts.

***Disclosures by whistleblowers.*** covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a UAB "Ligence" discloses protected health information, provided that:

The workforce member or UAB "Ligence" believes in good faith that covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by covered entity potentially endangers one or more patients, workers, or the public; and

The disclosure is to:

A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by covered entity; or

An attorney retained by or on behalf of the workforce member or UAB "Ligence" for the purpose of determining the legal options of the workforce member or UAB "Ligence" with regard to the conduct described as: The workforce member or UAB "Ligence" believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public.

**8.7.2. Uses and disclosures: Organizational requirements**

***Business associate contracts***

UAB "Ligence" is not in compliance with the standards in Disclosures to business associates, if UAB "Ligence" knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless UAB "Ligence" took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

A contract between the covered entity and UAB "Ligence" must:

Establish the permitted and required uses and disclosures of protected health information by UAB "Ligence". The contract may not authorize the UAB "Ligence" to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

- The contract may permit the UAB "Ligence" to use and disclose protected health information for the proper management and administration of the UAB "Ligence", as provided in paragraph Other requirements for contracts and other arrangements of this section; and
- The contract may permit the UAB "Ligence" to provide data aggregation services relating to the health care operations of the covered entity.

Provide that the UAB "Ligence" will:

- Not use or further disclose the information other than as permitted or required by the contract or as required by law;
- Use appropriate safeguards and comply, where applicable, with Security Standards for the Protection of Electronic Protected Health Information with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;
- Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by Notification by a business associate;
- Ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of UAB "Ligence" agree to the same restrictions and conditions that apply to UAB "Ligence" with respect to such information;
- Make available protected health information in accordance with Access of individuals to protected health information;
- Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with Amendment of protected health information;
- Make available the information required to provide an accounting of disclosures in accordance with Accounting of disclosures of protected health information;
- To the extent UAB "Ligence" is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.
- Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by UAB "Ligence" on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and
- At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by UAB "Ligence" on behalf of, the covered entity that UAB "Ligence" still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

Authorize termination of the contract by the covered entity, if the covered entity determines that UAB "Ligence" has violated a material term of the contract.

***Other arrangements***

If UAB "Ligence" is required to provide a service described in the definition of business associate to a covered entity, such covered entity may disclose protected health information to UAB "Ligence" to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and UAB "Ligence" contracts or other arrangements, if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph business associate contracts of this section and business associate contracts or other arrangements, if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

The covered entity may omit from its other arrangements the termination authorization required to Authorize termination of the contract by the covered entity, if the covered entity determines that the UAB "Ligence" has violated a material term of the contract, if such authorization is inconsistent with the statutory obligations of the covered entity or UAB "Ligence".

A covered entity may comply with business associate contracts or other arrangements. if the covered entity discloses only a limited data set to UAB "Ligence" for the UAB "Ligence" to carry out a health care operations function and the covered entity has a data use agreement with UAB "Ligence" that complies with Data use agreement and business associate contracts or other arrangements, if applicable.

***Other requirements for contracts and other arrangements***

The contract or other arrangement between the covered entity and UAB "Ligence" may permit UAB "Ligence" to use the protected health information received by UAB "Ligence" in its capacity as UAB "Ligence" to the covered entity, if necessary:

- For the proper management and administration of UAB "Ligence"; or
- To carry out the legal responsibilities of UAB "Ligence".

The contract or other arrangement between the covered entity and UAB "Ligence" may permit UAB "Ligence" to disclose the protected health information received by UAB "Ligence" in its capacity as UAB "Ligence" for the purposes described in paragraph Other requirements for contracts and other arrangements of this section, if:

- The disclosure is required by law; or
    - UAB "Ligence" obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and
    - The person notifies UAB "Ligence" of any instances of which it is aware in which the confidentiality of the information has been breached.

***Business associate contracts with subcontractors***

The requirements of UAB "Ligence" contracts through Other requirements for contracts and other arrangements apply to the contract or other arrangement between a UAB "Ligence" and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and UAB "Ligence".

**8.7.3. Other requirements relating to uses and disclosures of protected health information**

***Permitted purposes for uses and disclosures***

A covered entity may use or disclose a limited data set under paragraph Limited data set of this section only for the purposes of research, public health, or health care operations.

A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph Limited data set: of this section, or disclose protected health information only to UAB "Ligence" for such purpose, whether or not the limited data set is to be used by the covered entity.

***Fundraising communications***

***Uses and disclosures for fundraising***

A covered entity may use, or disclose to UAB "Ligence" or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of Uses and disclosures for which an authorization is required:

- Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;
- Dates of health care provided to an individual;
- Department of service information;
- Treating physician;
- Outcome information; and
- Health insurance status.

**8.7.4. Administrative requirements**

***Mitigation***

A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart (Privacy of Individually Identifiable Health Information) by the covered entity or UAB "Ligence".

**8.7.5. Transition provisions**

***Effect of prior contracts or other arrangements with business associate's***

Notwithstanding any other provisions of this part, a covered entity, or UAB "Ligence" with respect to a subcontractor, may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that comply with the administrative safeguards (see chapter 7. Administrative safeguards in accordance with 164.308(b), and with the requirements for business associate contracts or other arrangements (see chapter 8. Organizational requirements - business associate contracts or other arrangements in accordance with 164.314(a)).

**8.7.6. Administrative safeguards in accordance with 164.308(b)**

A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on this behalf only if the business associate obtains satisfactory assurances, that the subcontractor will appropriately safeguard the information.

Written contract or other arrangement. Document the satisfactory assurances through a written contract or other arrangement with the business associate.

**8.7.7. Organizational requirements - business associate contracts or other arrangements in accordance with 164.314(a)**

The contract must provide that business associate will:

- comply with the applicable requirements of the CFR subpart 164.314 "Organizational requirements";
- ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of the CFR subpart 164.314 "Organizational requirements" by entering into a contract or other arrangement; and
- report to the cover entity any security incident of which it becomes aware, including breaches of unsecured protected health information.

Business associate contracts with subcontractors must also apply above mentioned requirements in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.