Policy of processing and personal data protection

of the healthcare organization FSBI “Clinical sanatorium “Barviha” of the Administrative Department of the President of the Russian Federation

1. General provisions

1.1. Present policy in respect to personal data processing (hereafter referred to as Policy) is executed in accordance with item 2 art.18.1 of the Federal Law N152-FZ from July, 27th, 2006 “About personal data” and is a framework internal regulative document of the healthcare organization FSBI “Clinical sanatorium “Barviha” of the Administrative Department of the President of the Russian Federation (further hereafter designated Organization or Operator) which defines the key directions of its activity as per processing and personal data security (hereafter referred to as PD), Operator of which is Organization.

1.2. The policy is elaborated with the view to realize legal requirements in the field of processing and personal data security and is aimed to protect of human and civil rights and liberties while processing his PD in the Organization, including privacy law, personal, family and privacy of health-care providers.

1.3. Provisions of the Policy extend to relationships on PD processing and protection received by the Organization both before and after Policy validation, excluding the cases when Policy provisions cannot be applied to relationships on PD processing and protection received before its validation due to legal, organizational or some other characters.

1.4. Processing of the data in the Organization is realized in connection with implementation of the functions of the Organization as provided for by its constitutive documents and determined by:

- Federal Law dated November, 21st, 2011 N323 FZ “About fundamentals of health protection of the citizens of the Russian Federation”.
- Federal Law N 152-FZ dated July, 27th, 2006 “About personal data”
- Decree of the Russian Government dated September, 15th 2008 N687 “About approval of the provision of particular qualities of the personal data processing realized without use of automation facilities”;

- Decree of the Russian Government dated November, 1st 2012 “About approval requirements for the personal data security while their processing in personal data information systems”;
- Other pieces of legislation of the Russian Federation.

Besides that, personal data processing is carried out in the Organization in course of labor and other directly relating to them relationships where Organization acts as an employer (chapter 14 of the Labor Code of the Russian Federation) in connection with Organization realization of its rights and duties as a legal entity.

1.5. Organization has a right to make changes in the present policy. While doing that in the Policy headline one should indicate the date of the latest wording update. New Policy wording takes legal effect from the date of its allocation on the site, except as otherwise provided by the new Policy wording.

1.6. Current version is kept in the registered office of the Organization with an address at: Moscow region, Odintsovsky district, station Barviha, electronic version of the Policy – at the following URL: http://www.barvihamed.ru

2. Terms and authorized abbreviations

Personal data (PD) – any information related to specifically or implied established or defined physical party (personal data owner);

Personal data processing – any action (operation) or cumulative action (operation) executed using automation facilities or without use of such tools with personal data including collection, recording, classification, accumulation, storage, refinement (updating, change), retrieval, usage, disclosure (distribution, submission, access), depersonalization, blocking, deleting, destruction of the personal data.

Operator – government body, municipal authority, legal or natural person, independently or together with other persons organizing and (or) performing personal data processing as well as defining objections of personal data processing, scope of personal data, being a subject to processing; actions (operations) accomplished with personal data.

Personal data diffusion – actions intended to personal data disclosure to the public;

Personal data submission – actions intended to personal data disclosure to a certain person or certain group of persons;

Personal data blocking - abeyancy of the personal data processing (except in cases of necessity of the processing for personal data rectification);

Personal data destruction – actions, as a result of which it is impossible to restore personal data content in the information system of the personal data and (or) as a result of which material objects of personal data are destructed;

Personal data depersonalization – actions, as a result of which it is impossible to identify personal data affiliation to the specific subject of personal data without usage of additional information;

Automated personal data processing – personal data processing with the help of means of computer technology;

Information system of personal data (ISPD) – pooled personal data in the data bases and ensuring their processing of the information technologies and technical means;

Patient – physical person to whom health care is delivered or who applied for the medical care delivery regardless whether he has a disease or his state;

Medical activity – professional activity on health care delivery, carrying out expert medical examinations, medical surveys and medical certification, sanitary-antiepidemic (preventing) measures and professional activity, connected to organ transplantation (grafting) and (or) tissue transfer, donated blood transformation and (or) its components medicinally;

Consulting physician – a doctor who performs functions of organization and direct health care delivery to a patient within the period of the treatment and monitoring;

3. Principles of personal data safety provision

3.1. The main task of the safety provision of PD while their processing in Organization is unauthorized access to them of the third party, caution of intended programmed-technical and other impacts with the aim of identity theft, disruption (elimination) or their distortion during data processing.

3.2. To ensure PD security Organization applied the following principles:

- legality: PD protection is based on provisions of the legislative instruments and guidelines documents authorized governmental entities in the sphere of PD processing and protection;
- consistency: PD processing in the Organization is performed taking into account all interrelated interactive and time dependent elements, conditions and factors meaningful to realize and settle the problem of PD safety maintenance;

- integrity: PD protection is done with usage of functional possibilities of the information technologies, realized in the information systems of the Organization and other available systems and means of protection of the Organization;
- continuity: PD protection is ensured on all the stages of their processing and in all the regimes of functioning of the PD processing systems including maintenance and scheduled operations;
- timeliness: measures, ensuring the proper level of PD security are taken before their processing;
- continuity of upgrading: modernization and buildup of measures and PD safety measures is realized on the base of analyses of the results of PD processing in the Organization taking into account identifying of the new means and facilities realizing PD security threats as well as home and foreign experience in the sphere of info protection;
- personal responsibility: employees are rendered liable for the PD security maintenance within their responsibilities in connection with PD processing and protection;
- minimization of the access rights: access to PD is rendered to Employees only in the volume necessary for implementation of their official duties;
- flexibility: enforcement of the PD security functions at changing characteristics of the functioning of the information systems of the personal data of Organization, as well as the volume and contents of the PD processing;
- specialization and professionalism: realization of the measures on PD security provision is performed by Employees having necessary for this qualification and experience;
- efficiency of recruitment process: recruitment policy of Organization provides thorough staff recruitment and motivation of the Employees which allows to eliminate or minimize possibility of their violation of PD security;
- observability and transparency: measures on PD security maintenance should be planned so the results of their application are apparently visible (transparent) and can be evaluated by persons carrying out control;
- continuity of control and evaluation: procedures of the permanent control of the usage of systems of PD processing and protection are implemented, and the results of the control are regularly analyzed.

3.3. PD processing unsuitable for their collection aims is not carried out in the Organization. Unless otherwise stipulated by Federal law, upon completion of PD processing in the Organization, as well as achieving goals of their processing or in case

of no further need in achieving these goals, PD processed by Organization are eliminated or depersonalized.

3.4. While PD processing data accuracy and sufficiency is ensured, and if necessary – their actuality in regards to the purposes of processing. Organization takes necessary measures on elimination or qualification of incomplete or imperfect PD.

4. Personal data processing

4.1. PD acquisition

4.1.1. All PD should be received from a person first-hand. If PD of a person can be acquired only from the third party then a person should be informed about it and one should get consent from the person.

4.1.2. Operator should inform a person about aims, implied sources and ways of PD acquisition, features of the acquired PD, action plan with PD, term within which his consent is valid and order of withdrawal of consent, as well as consequences of person's refusal to give a written consent for their acquisition.

4.1.3. Documents containing PD are composed by way of:

a) original documents copying (passport, document about education, Individual Taxpayer Number certificate, pension certificate, etc.);

b) making entries on stock record cards;

c) acquisition of the originals of the necessary documents (work record book, medical evidence, personal reference, etc.).

PD access procedure of a subject to his processing in Organization is defined due to legislation and governed by internal regulating documents of the Organization.

4.2. PD processing

4.2.1. Personal data processing is conducted:

- upon consent of the personal data subject for his personal data processing;
- in cases when personal data processing is necessary for realization and implementation of functions, powers, and duties vested by Russian Federation legislation;
- in cases when personal data processing is performed, to which access of unlimited scope of persons is rendered by the subject of personal data or by his request (further- personal data, made public by the subject of personal data).

Employees' access to the processing PD is carried out in accordance with their official duties and requirements of the internal regulating documents of the Organization.

Having access to the PD processing Employees against signature get acquainted with the documents, establishing order of PD processing including documents, establishing rights and duties of the specified Employees.

Organization performs elimination of the revealed violations of legislation of PD processing and protection.

4.2.2 Purposes of PD processing.

- maintenance of health care organization for the population as well as more complete enforcing obligations and competences due to Federal Law dated November , 21st N 323-FZ “About fundamentals of health protection of the citizens of the Russian Federation” dated November, 29th 2010, N 326-FZ “About drug circulation” and dated November, 29th, 2010 N 326-FZ “About compulsorry health insurance of the citizens of the Russian Federation”, rules of rendering by health organizations of payable health care services, approved by government Decree from October, 4th 2012 N 1006;
- performance of working relations;
- performance of civil law relations.

4.2.3. Categories of the personal data subjects

Organization processes personal data of the following subjects:

- physical persons who are in working relationships;
- physical persons close relatives of the employees of the institution;
- physical persons retired from the institution;
- physical persons who are potential employees;
- physical persons who are in civil law relations with the institution;
- physical persons who applied for health care to the institution.

4.2.4. Personal data processed by Organization

- data received at working relations;
- data received for selection of the candidates for work in organization;
- data received at fulfillment of the civil law relations;
- data received at health care delivery.

The full list of PD is presented in the List of PD, approved by the Chief Doctor of the Organization.

4.2.5. Personal data processing is carried out:

- with usage of automatic means;
- without usage of automatic means.

4.3. PD storage

4.3.1. PD of the subjects can be received further processed and revert to stock both in electronic and paper form.

4.3.2. PD fixed on paper is stored in lockers or locked premises with limited access (register office).

4.3.3. PD of the subjects processed with automatic means with different aims is stored in different files (page).

4.3.4. It is not allowed to store and allocate documents with PD in open electronic catalogues (share sites) in ISPD.

4.3.5. PD storing in a form that allows defining PD subject is realized not longer than it is needed for the purposes of processing; and it is liable to destruction upon achieving the aims of processing or if there is no necessity to achieve them.

4.4. PD destruction

Destruction of the documents (media) that contain PD is done by burning, crush (fragmentation), chemical decomposition, turning into formless mass or powder. Paper documents can be eliminated in a shredding machine.

4.4.2. PD on electronic media is destructed by deleting or media formatting.

4.4.3. Destruction is carried out by a commission. Fact of PD destruction is confirmed by a document about media destruction signed by members of the commission.

4.5. PD disclosure

4.5.1. Organization discloses PD to a third party in the following cases:

- a person expressed his consent for such actions;
- disclosure is provided by applicable law to the extent permitted by the applicable law.

4.5.2. List of persons to whom PD is disclosed

Third parties to whom PD is disclosed:

- Pension fund of the Russian Federation for registration (legally);
- Tax services of the Russian Federation (legally);
- Social Insurance Fund (legally);
- Territorial fund of the compulsory health insurance (legally);
- Insurance health organizations on compulsory and voluntary medical insurance (legally);
- Banks for payroll calculation (pursuant to an Agreement);
- Judicial and law enforcement authorities in cases, established by legislation;
- Credit terms bureau (upon person’s consent);

- Judicial companies working within the limits of legislation of the Russian Federation in cases of credit contract failure of performance (upon person's consent).

5. Personal data protection

5.1. The system of personal data protection (SPPD) is created due to the requirements of the ruling documents of the Organization; it consists of subsystems of legal, organizational and technical protections.

5.2. Subsystem of the legal protection represents complex of legal, organizational/management and ruling documents ensuring creation, functioning and perfection of SPPD.

5.3. Subsystem of organizational protection includes organization of the structure of SPPD management, authorization system, and information protection when working with employees, partners and third parties, information protection in public mass media, public and advertising activity, analytical work.

5.4. Subsystem of technical protection includes complex of technical, programming tool, soft hardware ensuring PD protection.

5.5. Main PD protection measures used in Organization are:

5.5.1. Assignment to a position of a person in charge for PD processing, who performs organization of PD processing, training and instruction, internal control of the institution and its employees as per compliance with the requirements to PD protection;

5.5.2. Determination of the actual security threat at its processing in SPPD, and measures and arrangements' development protecting PD.

5.5.3. Policy development regarding to PD processing.

5.5.4. Regulation rules for PD accessibility processed in SPPD as well as registration and recording of all the actions performed with PD in SPPD.

5.5.5. Setting of Individual access passes of the employees for the information system in accordance to their working duties.

5.5.6. Appliance of the means of information protection which passed the estimation procedure in due order, PD media-resident software and insurance of its safety.

5.5.7. Certified antivirus software with regularly updating bases.

5.5.8. Certified software for information protection against unauthorized access.

5.5.9. Certified fire wall and intrusion detector.

5.5.10. Observance of terms providing PD safety and excluding unauthorized intrusion, estimation of efficiency of the measures taken and realized to ensure PD safety.

5.5.11. Regulation of access rules to the processed PD, maintenance of registration and recording of the actions performed with PD, as well as revealing of the facts of unauthorized access to personal data and taking measures.

5.5.12. PD restoration modified or destructed because of unauthorized access to them.

5.5.13. Training of the employees of the Organization performing first-hand personal data processing of the provisions of the legislation of the Russian Federation about personal data, including requirements for personal data protection with the policy-making documents of the Organization in regards with personal data processing, internal acts regarding personal data processing.

5.5.14. Performing of internal control and auditing.

6. Basic rights of the PD subject and duties of Organization

6.1. Basic rights of the PD subject

PD subject has a right to receive information regarding his personal data processing, which includes:

- confirmation of the personal data processing by an operator;
- legal bases and purposes of the personal data processing;
- aims and ways of personal data processing applicable by an operator;
- name and address of an operator, information about persons (excluding employees of the operator) who has an access to personal data or to whom personal data can be disclosed due to the agreement with the operator or under the federal law;
- processed personal data related to corresponding subject of personal data, its source, except as otherwise permitted by applicable federal law;
- terms of personal data processing, including terms of its storage;
- procedure for the exercise of the right of the personal data subject legally provided by the federal law “ About personal data”
- information about performed or supposed cross-border data transmission;

- name or second name, first name, address of a person performing personal data processing on an errand of the operator, if the processing is assigned or will be assigned to such a person;
- any other information, legally provided by the federal law or other federal laws.

PD subject has a right to demand from the operator personal data refinement, its blocking or destruction in case if personal data is not complete, out of date, inaccurate, received illegally, or is not needful for the declared purpose of processing; as well as to take measures legally provided to protect his rights.

6.2. Duties of Organization

Organization is obliged:

- while collecting PD present information about his PD processing;
- in cases if PD were received not from the subject inform him;
- at refusal to present PD, consequences of such refusal are explained to a subject;
- publish or by any other way provide unlimited access to the document determining policy with regards to PD, to the information about implemented requirements to PD protection;
- take necessary legal, organizational and technical measures or provide their application to protect PD against illegal or casual access, destruction, amendment, blocking, copying, presenting, distribution of the PD or other illegal actions regarding PD;
- give replies to requests and applications of the PD subjects, their representatives and authorized body on protection of the PD subjects' rights.