

Приложение № 1
к приказу главного врача
ГКУЗ «ККПБ им. В.Х.Кандинского»
от 14 ноября 2022г. №633

ПОЛОЖЕНИЕ

**в области обработки и защиты персональных данных работников
и пациентов в государственном казённом учреждении
здравоохранения "Краевая клиническая психиатрическая больница
имени В.Х. Кандинского"**

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение в области обработки и защиты персональных данных работников и пациентов (далее - Положение) разработано с целью обработки и защиты информации, относящейся к личности работников и пациентов государственного казённого учреждения здравоохранения "Краевая клиническая психиатрическая больница имени В.Х. Кандинского" (далее – Оператор, Больница), в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, законодательными актами Российской Федерации об охране здоровья граждан, Законом Российской Федерации «О психиатрической помощи и гарантиях прав граждан при ее оказании» от 2 июля 1992 года № 3185-1, Постановлением Правительства Российской Федерации от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации", Постановлением Правительства Российской Федерации от 21.03.2012 № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами", Указом Президента Российской Федерации от 06.03.1997г. № 188 "Об утверждении Перечня сведений конфиденциального характера".

2. ОСНОВНЫЕ ПОНЯТИЯ

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (это могут быть фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация);

персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц, к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника;

персональные данные пациента - информация, необходимая Больнице в связи с отношениями, возникающими между пациентом, его законными представителями и Больницей, в том числе информация, составляющая врачебную тайну;

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. СВЕДЕНИЯ ОБ ОПЕРАТОРЕ

3.1 Государственное казённое учреждение здравоохранения "Краевая клиническая психиатрическая больница имени В.Х. Кандинского" зарегистрировано в реестре операторов персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

3.2 Оператор ведет свою деятельность по адресам:

- Забайкальский край, г. Чита, Окружной проезд, дом 3;
- Забайкальский край, г. Чита, ул.Амурская, дом 97;
- Забайкальский край, г. Чита, ул.Староивановская, дом 45.

3.3 Базы данных информации, содержащей персональные данные граждан Российской Федерации, находятся по адресам:

- Забайкальский край, г. Чита, Окружной проезд, дом 3;
- Забайкальский край, г. Чита, ул.Амурская, дом 97;
- Забайкальский край, г. Чита, ул.Староивановская, дом 45.

3.4 Доступ к персональным данным субъектов персональных данных имеют сотрудники государственного казённого учреждения здравоохранения "Краевая клиническая психиатрическая больница имени В. Х. Кандинского" в рамках исполнения своих должностных обязанностей.

4. СУБЪЕКТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

К субъектам персональных данных в государственном казённом учреждении здравоохранения "Краевая клиническая психиатрическая больница имени В. Х. Кандинского" относятся следующие категории физических лиц:

- 1) работники Больницы;
- 2) близкие родственники работников Больницы, персональные данные которых необходимы в целях выполнения требований трудового законодательства Российской Федерации;
- 3) физические лица, с которыми заключен договор гражданско-правового характера;
- 4) физические лица, с которыми заключен договор об обучении;
- 5) граждане, обратившиеся за медицинской помощью (пациенты Больницы);

б) законные представители/близкие родственники граждан, обратившихся за медицинской помощью.

5.СВЕДЕНИЯ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Оператор обрабатывает персональные данные на законной и справедливой основе для выполнения возложенных законодательством функций, полномочий и обязанностей, осуществления прав и законных интересов Оператора, работников и пациентов Оператора и третьих лиц.

5.2. Оператор получает персональные данные непосредственно от субъектов персональных данных или их законных представителей.

5.3. Оператор обрабатывает персональные данные автоматизированным, неавтоматизированным способами, с использованием средств вычислительной техники и без использования таких средств.

5.4. Действия по обработке персональных данных включают сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение.

5.5. Базы данных информации, содержащей персональные данные граждан Российской Федерации, находятся на территории Российской Федерации.

6.СОГЛАСИЕ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБРАБОТКУ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1 Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

6.2 Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

6.3 В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

6.4 В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

6.5 В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Оператором.

6.6 Согласие на обработку персональных данных субъектов персональных данных может быть дано субъектом персональных данных в любой позволяющей подтвердить факт его получения форме. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

6.7 Если персональные данные получены не от субъекта персональных данных, Оператор, за исключением случаев, предусмотренных пп.6.3-6.5 настоящего Положения, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

2) цель обработки персональных данных и ее правовое основание;

3) предполагаемые пользователи персональных данных;

4) установленные законом права субъекта персональных данных;

5) источник получения персональных данных.

6.8 Согласие на обработку персональных данных может быть отозвано субъектом персональных данных по письменному запросу. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии законных оснований (ст.10 п.15 Федерального закона от 30.12.2020г. № 519-ФЗ.).

6.9 Ограничение прав пациентов Больницы на защиту своих персональных данных только на основании психиатрического диагноза, фактов нахождения под психиатрическим наблюдением не допускается. Пациенту, как субъекту персональных данных, информация о своих правах должна быть предоставлена в доступной форме и с учетом его психического состояния.

7.ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

7.1. Оператор обрабатывает персональные данные работников в рамках правоотношений, урегулированных Трудовым Кодексом Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (далее — ТК РФ), в том числе главой 14 ТК РФ, касающейся защиты персональных данных работников.

7.2. Оператор обрабатывает персональные данные работников с целью выполнения трудовых договоров, соблюдения норм законодательства РФ, а также с целью:

— вести кадровый учёт;

— вести бухгалтерский учёт;

— осуществлять функции, полномочия и обязанности, возложенные законодательством РФ на Оператора, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд РФ, а также в иные государственные органы;

— соблюдать нормы и требования по охране труда и обеспечения личной безопасности работников государственного казённого учреждения здравоохранения "Краевая клиническая психиатрическая больница имени В. Х. Кандинского";

— сохранности имущества работодателя;

- контролировать количество и качество выполняемой работы работником;
- предоставлять льготы и компенсации, предусмотренные законодательством РФ;
- организовывать обучение работников государственного казённого учреждения здравоохранения "Краевая клиническая психиатрическая больница им. В. Х. Кандинского";
- предоставление отчетности в ПФР, ФНС и иные органы.

7.3. Оператор не принимает решения, затрагивающие интересы работников, основываясь на их персональных данных, полученных электронным образом или исключительно в результате автоматизированной обработки.

7.4. Оператор защищает персональные данные работников за счет собственных средств в порядке, установленном ТК РФ, ФЗ «О персональных данных» и иными федеральными законами.

7.5. Оператор знакомит работников и их представителей под роспись с документами, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

7.6. Оператор разрешает доступ к персональным данным работников только допущенным лицам, которые имеют право получать только те данные, которые необходимы для выполнения их функций.

7.7. Оператор получает все персональные данные работников у них самих. Если данные о работнике возможно получить только у третьей стороны, Оператор заранее уведомляет об этом работника и получает его письменное согласие. Оператор сообщает работнику о целях, источниках, способах получения, а также о характере подлежащих получению данных.

7.8. Оператор обрабатывает персональные данные работников с их письменного согласия.

7.9. Оператор обрабатывает персональные данные работников в течение срока действия согласия на обработку персональных данных. Оператор обрабатывает персональные данные уволенных работников в течение срока, установленного п. 5 ч. 3 ст. 24 части первой Налогового Кодекса Российской Федерации от 31 июля 1998 г. № 146-ФЗ, ч. 1 ст. 29 Федерального закона «О бухгалтерском учёте» от 6 декабря 2011 г. № 402-ФЗ и иными нормативными правовыми актами.

7.10. Оператор может обрабатывать специальные категории персональных данных работников (сведений о состоянии здоровья, относящихся к вопросу о возможности выполнения ими трудовых функций) на основании п. 2.3 ч. 2 ст. 10 ФЗ «О персональных данных».

7.11. Оператор обрабатывает биометрические персональные данные работников, используя системы видеонаблюдения с хранением видеозаписей в сроки, установленные законодательством Российской Федерации в кабинетах, коридорах, лестничных клетках и на территории работодателя (цветное и черно-белое цифровое фотографическое изображение; цветное и черно-белое цифровое видеоизображение). Цель получения биометрических персональных данных – обеспечение безопасности на территории ГКУЗ «ККПБ имени В.Х. Кандинского»; контроль выполнения работниками правил внутреннего трудового распорядка.

7.12. Оператор не получает данные о членстве работников в общественных объединениях или их профсоюзной деятельности, за исключением случаев, предусмотренных ТК РФ или иными федеральными законами.

7.13. Оператор обрабатывает следующие персональные данные работников:

- Фамилия, имя, отчество;
- Тип, серия и номер документа, удостоверяющего личность;
- Дата выдачи документа, удостоверяющего личность, и информация о выдавшем его органе;
- Дата рождения;
- Место рождения;
- Адрес регистрации, адрес фактического проживания;
- Номер контактного телефона;
- Идентификационный номер налогоплательщика;
- Номер страхового свидетельства государственного пенсионного страхования;
- Семейное положение;
- Образование, данные документов об образовании;

- Профессия;
- Доходы;
- Страховые взносы на ОПС;
- Страховые взносы на ОМС;
- Налоговые вычеты;
- Социальные льготные выплаты;
- Выход на пенсию;
- Временная нетрудоспособность;
- Должность;
- Табельный номер;
- Трудовой стаж;
- Учёная степень, звание;
- Банковские реквизиты;
- Анкетные данные, заполняемые работником при поступлении на работу или в процессе работы (в том числе автобиография);
- Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);

7.14. Оператор не сообщает третьей стороне персональные данные работника без его письменного согласия, кроме случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных ТК РФ, ФЗ «О персональных данных» или иными федеральными законами.

7.15. Оператор не сообщает персональные данные работника в коммерческих целях без его письменного согласия.

7.16. Оператор передаёт персональные данные работников их представителям в порядке, установленном ТК РФ, ФЗ «О персональных данных» и иными федеральными законами, и ограничивает эту информацию только теми данными, которые необходимы для выполнения представителями их функций.

7.17. Оператор предупреждает лиц, получающих персональные данные работника, что эти данные могут быть использованы только в целях, для которых они сообщены, требует от этих лиц подтверждения, что это правило соблюдено.

7.18. В порядке, установленном законодательством, и в соответствии со ст. 7 ФЗ «О персональных данных» для достижения целей обработки персональных данных и с согласия работников Оператор предоставляет персональные данные работников следующим лицам:

- Государственные органы (ПФР, ФНС, военные комиссариаты);
- Банк (в рамках зарплатного проекта).

7.19. Работник может получить свободный бесплатный доступ к информации о его персональных данных и об обработке этих данных. Работник может получить копию любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных федеральным законом.

7.20. Работник может получить доступ к медицинской документации, отражающей состояние его здоровья, с помощью медицинского работника по его выбору.

7.21. Работник может определить представителя для защиты его персональных данных.

7.22. Работник может требовать исключить или исправить свои неверные или неполные персональные данные, а также данные, обработанные с нарушением требований ТК РФ, ФЗ «О персональных данных» или иного федерального закона. При отказе Оператора исключить или исправить персональные данные работника он может заявить в письменной форме о своем несогласии и обосновать такое несогласие. Работник может дополнить персональные данные оценочного характера заявлением, выражающим его собственную точку зрения.

7.23. Работник может требовать известить всех лиц, которым ранее были сообщены его неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

7.24. Работник может обжаловать в суде любые неправомерные действия или бездействие Оператора при обработке и защите его персональных данных.

8. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ФИЗИЧЕСКИХ ЛИЦ: «ЧЛЕНЫ СЕМЬИ РАБОТНИКОВ»

8.1. Оператор обрабатывает персональные данные физических лиц «члены семьи работников» в рамках правоотношений с Оператором.

8.2. Оператор обрабатывает персональные данные физических лиц «члены семьи работников» с целью:

— осуществлять виды деятельности, предусмотренные учредительными документами Государственного казённого учреждения здравоохранения "Краевая клиническая психиатрическая больница имени В. Х. Кандинского".

8.3. Оператор обрабатывает персональные данные физических лиц «члены семьи работников» с их согласия, предоставляемого в письменной форме.

8.4. Оператор обрабатывает персональные данные физических лиц «члены семьи работников» не дольше, чем того требуют цели обработки персональных данных, если иное не предусмотрено требованиями законодательства РФ.

8.5. Оператор обрабатывает специальные категории персональных данных несовершеннолетних физических лиц «члены семьи работников» с письменного согласия их законных представителей.

8.6. Оператор обрабатывает следующие персональные данные физических лиц «члены семьи работников»:

- Фамилия, имя, отчество;
- Пол, возраст;
- Тип, серия и номер документа, удостоверяющего личность;
- Дата выдачи документа, удостоверяющего личность, и информация о выдавшем органе;
- Дата рождения;
- Место рождения;
- Адрес регистрации и адрес фактического проживания.

9. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ БОЛЬНИЦЫ

9.1. Оператор обрабатывает персональные данные пациентов в соответствии с Конституцией Российской Федерации, законодательными актами Российской Федерации об охране здоровья граждан, Законом Российской Федерации «О психиатрической помощи и гарантиях прав граждан при ее оказании» от 2 июля 1992 года № 3185-1.

9.2. Обработка персональных данных пациентов осуществляется исключительно в целях защиты их жизни, здоровья или иных жизненно важных интересов других лиц.

9.3. К персональным данным пациентов (их законных представителей), получаемыми Больницей и подлежащими хранению в Больнице в порядке, предусмотренном действующим законодательством и настоящим Положением, относятся следующие сведения, содержащиеся в стационарных и амбулаторных медицинских картах:

- фамилия, имя, отчество пациента (законного представителя);
- дата рождения пациента (законного представителя);
- место жительства пациента (законного представителя);
- данные полиса медицинского страхования;
- СНИЛС;
- контактный телефон пациента (законного представителя);
- место работы, должность пациента (законного представителя);
- паспортные данные пациента (законного представителя) или данные, содержащиеся в свидетельстве о рождении;
- данные о состоянии здоровья при поступлении/постановке на учет (диагноз, сведения об инвалидности, о беременности, результаты диагностических исследований и пр.);
- данные, заполняемые при ведении медицинских карт (направление на лечение, дата поступления/выписки, добровольная/недобровольная госпитализация, диагноз, исход заболевания, результаты проведенных экспертиз, результаты дополнительных методов обследования и пр.);
- постановления суда о признании недееспособным, решения о назначении опекуна.

9.4. Все персональные данные пациента предоставляются самим пациентом. Персональные данные несовершеннолетнего в возрасте до 15 лет предоставляются его родителями или иными законными представителями. Персональные данные лица, признанного в установленном законом порядке недееспособным, предоставляются его законным представителем.

9.5. Обработка персональных данных пациента может осуществляться только с его согласия в письменной форме, для несовершеннолетнего в возрасте до 15 лет согласие в письменной форме дают его родители или законные представители. В случае недееспособности субъекта персональных данных (пациента) согласие на обработку его персональных данных дает в письменной форме его законный представитель.

9.6. Допускается обработка персональных данных без согласия пациента:

- в целях обследования и лечения гражданина, не способного из-за своего состояния выразить свою волю;
- в целях обследования и лечения гражданина, непосредственно опасного для себя и окружающих;
- в рамках оказания психиатрической помощи гражданину в случае, если оставление его без такой помощи приведет к существенному ухудшению психического состояния;
- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- по запросу органов дознания и следствия, прокурора и суда в связи с проведением расследования или судебным разбирательством;
- в случае оказания помощи несовершеннолетнему в возрасте, установленном ст. 24 Основ законодательства Российской Федерации об охране здоровья граждан (утв. ВС РФ 22.07.1993 N 5487-1) (больные наркоманией в возрасте старше 16 лет, иные несовершеннолетние в возрасте старше 15 лет), для информирования его родителей или законных представителей;
- при наличии оснований, позволяющих полагать, что вред здоровью гражданина причинен в результате противоправных действий;
- в целях проведения военно-врачебной экспертизы в порядке, установленном положением о военно-врачебной экспертизе, утвержденным Правительством Российской Федерации.

9.7. Персональные данные пациента о состоянии его здоровья передаются третьим лицам без согласия субъекта персональных данных или его законного представителя (ч. 4 ст. 13 Закона № 323-ФЗ):

- если пациент в результате своего состояния не способен выразить свою волю, но ему необходимо лечение;
- при угрозе распространения инфекционных заболеваний, массовых отравлений;
- по запросу органов дознания и следствия, суда, органа уголовно-исполнительной системы;
- в случае оказания медицинской помощи несовершеннолетнему;
- в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются основания полагать, что вред его здоровью причинен в результате противоправных действий;
- в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов;
- при обмене информацией медицинскими организациями, в т.ч. размещенной в информационных системах, в целях оказания медицинской помощи;
- в целях осуществления учета и контроля в системе обязательного социального страхования;
- в целях осуществления контроля качества и безопасности медицинской помощи.

9.8. Письменное согласие пациента на передачу (предоставление) его персональных данных, составляющих врачебную тайну, требуется в случаях, когда:

- медицинская помощь оказывается пациенту на платной основе, вне программы государственных гарантий, и сведения передаются третьим лицам (организациям), не являющимся медицинскими организациями, например в страховую компанию;
- информация о состоянии здоровья пациента передается лицам, указанным самим пациентом или его законным представителем в информированном добровольном согласии на медицинское вмешательство (ч. 5 ст. 19 Закона № 323-ФЗ); в согласии должны быть

указаны фамилия, имя, отчество и контактные данные этих лиц;

- передача персональных данных (документов) пациента осуществляется по открытым каналам связи (сети Интернет, электронной почте), например, при проведении дистанционных (телемедицинских) консультаций;

- осуществляется трансграничная передача персональных данных пациента.

10. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Для реализации своих прав и законных интересов субъекты персональных данных имеют право обратиться к Оператору либо направить запрос лично или с помощью представителя.

10.2. Субъект персональных данных имеет право на получение информации (за исключением информации об осуществленной или предполагаемой трансграничной передаче данных) в доступной форме, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- способы обработки персональных данных, применяемые Оператором;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен доступ на основании договора или федерального закона;
- перечень обрабатываемых персональных данных субъекта и источник их получения;
- сроки обработки персональных данных и сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ «О персональных данных»;

10.3. Субъект персональных данных вправе требовать от Оператора уточнения своих персональных данных, блокирования или их уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

10.4. Субъект персональных данных вправе принимать предусмотренные законом меры по защите своих прав.

10.5. Повторно субъект может обратиться не ранее, чем через тридцать дней после первоначального обращения. Если предоставленные сведения были неполными, то субъект может обратиться повторно до истечения тридцати дней. Обращение должно содержать обоснование направления повторного обращения.

11. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Запрещается обрабатывать персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, частной жизни, членстве в общественных объединениях, профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

11.2. Запрещается располагать информацию, содержащую персональные данные, в папках общего доступа (`\\DATA\Public`).

11.3. Запрещается передавать информацию о персональных данных по открытым каналам связи без организации мер безопасности, на адреса личной электронной почты, с помощью мессенджеров.

12. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ ОПЕРАТОРОМ

12.1. Оператор при обработке персональных данных работников и пациентов принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий, в частности:

- работники, в должностные инструкции которых входит обработка персональных данных, подписывают Обязательство о неразглашении персональных данных и Обязательство о прекращении обработки персональных данных в случае расторжения с ними трудового договора;
- определение перечня персональных данных для каждой категории субъектов персональных данных;
- ограничение доступа к персональным данным путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- организация учета машинных носителей персональных данных
- в помещения, где ведется обработка персональных данных, допускаются только работники, уполномоченные на обработку персональных данных в соответствии с Приказом о допуске и внесенные в Списки должностных лиц, имеющих право нахождения в помещении.
- применение мер технической защиты информации.
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

13.ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

13.1. Персональные данные работников и пациентов Больницы хранятся на территории Российской Федерации

13.2. Персональные данные работников и пациентов Больницы хранятся на зарегистрированных бумажных носителях и учтенных электронных носителях отдельно в специально предназначенных для этого шкафах и помещениях. Шкафы и помещения отвечают требованиям обеспечения физической сохранности, находящейся в них документации и технических средств обработки информации, содержащей персональные данные. Организация режима обеспечения безопасности в таких помещениях исключает возможность неконтролируемого проникновения или пребывания в них посторонних лиц.

13.3. В процессе хранения персональных данных работников и пациентов Больницы должны обеспечиваться:

- требования нормативных документов, устанавливающих правила обработки персональных данных;
- сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации, настоящим Положением и другими нормативными документами;
- своевременное обнаружение фактов разглашения информации, содержащей персональные данные.

13.4. Доступ к персональным данным работников и пациентов Больницы должны иметь только специально уполномоченные лица, определенные соответствующим приказом по Больнице. При этом данные лица имеют право получать только те персональные данные, которые необходимы им для выполнения своих должностных обязанностей.

13.5. Сроки хранения персональных данных на бумажных носителях работников государственного казенного учреждения здравоохранения «Краевая психиатрическая больница имени В.Х. Кандинского» по каждому виду документов определяются в соответствии с Приказом Росархива от 20.12.2019 № 236 "Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения".

13.6. Сроки хранения персональных данных на бумажных носителях лиц, получивших медицинские услуги в государственном казенном учреждении здравоохранения «Краевая

психиатрическая больница имени В.Х. Кандинского» определяются в соответствии с Приказом Росархива от 20.12.2019 № 236 "Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения" и требованиями нормативно-правовых актов Министерства здравоохранения Российской Федерации.

13.7. Сроки хранения персональных данных в электронной форме определяются в соответствии с требованиями к срокам хранения персональных данных или по достижению цели обработки персональных данных.

13.8. Каждую неделю необходимо создавать резервную копию электронной базы и хранить на флеш-носителе или внешнем жестком диске.

13.8. Порядок хранения персональных данных и требования к местам хранения закреплен в локальных актах.

14. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

14.1. Уничтожение персональных данных субъекта осуществляется в следующих случаях:

- истек срок хранения документов;
- достигли цели обработки;
- выявили факт неправомерной обработки;
- работник отозвал согласие на обработку;
- работник направил требование прекратить обработку;
- работник направил требование прекратить распространение.

14.2. Порядок уничтожения документов закреплен в локальном акте.

14.3. Обработываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

14.4. Уничтожение обработанных персональных данных производится комиссией с составлением соответствующего акта.

14.5. Составляются сводные описи, согласованные с экспертной комиссией, персональных данных, подлежащих уничтожению за соответствующий период.

14.6. Результат отбора документов, содержащих персональные данные к уничтожению, оформляются актом о выделении к уничтожению документов, не подлежащих хранению. Акт о выделении к уничтожению документов, не подлежащих хранению, составляется и утверждается Оператором.

14.7. После утверждения актов о выделении к уничтожению документов, содержащих персональные данные, не подлежащих хранению, документы передаются на переработку (утилизацию) по акту об уничтожении персональных данных, в котором указываются дата передачи, количество сдаваемых документов, способ уничтожения документов, дата уничтожения, подписи лиц, уничтоживших документы.

14.8. Персональные данные на бумажном носителе уничтожаются путем сжигания, измельчения. Персональные данные на электронном носителе уничтожаются с помощью программных средств для уничтожения информации на магнитных носителях.

14.9. Акт об уничтожении персональных данных хранится согласно Приказа Росархива от 20.12.2019 № 236 "Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения".

15. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТА ТРЕТЬИМ ЛИЦАМ

15.1. При передаче персональных данных субъектов персональных данных

(работников и пациентов) уполномоченными сотрудниками Больницы должны соблюдаться следующие требования:

- не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в других случаях, предусмотренных нормативно-правовыми актами законодательства;
- не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные субъекта персональных данных, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта персональных данных, обязаны соблюдать их конфиденциальность.

15.2. Передача персональных данных пациентов осуществляется в соответствии с законодательством Российской Федерации и локальными нормативными актами. Лица, получающие персональные данные пациентов в связи с исполнением своих должностных обязанностей, обязаны соблюдать их конфиденциальность и использовать такие данные лишь в целях, для которых они были сообщены.

15.3. Без письменного разрешения работников и пациентов Больницы информацию конфиденциального характера можно передавать третьим лицам только в случаях, предусмотренных федеральными законами, а также если жизни и здоровью субъекта что-то угрожает.

15.4. Передача и обработка персональных данных третьими лицами проводится без согласия в следующие организации: пенсионный фонд (ст. 9 Федерального закона 01.04.1996 № 27-ФЗ), налоговые органы (ст. 24 НК РФ), военные комиссариаты (ст.4 Федерального закона от 28.03.1998 № 53-ФЗ), иные органы, если обязанность передачи таких сведений, относящихся к информации конфиденциального характера, закреплена соответствующими законами или же необходима для достижения установленных законами целей.

16.ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

16.1. Персональные данные при обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

16.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых, заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

16.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

16.4 При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

- а) типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств

автоматизации, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых, заведомо не совместимы.

16.5 При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения части персональных данных уничтожается материальный носитель с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

16.6 Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

16.7 Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

17.ОСУЩЕСТВЛЕНИЕ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оператор определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, который действует постоянно.

17.1. Определяется тематика проверок:

А)Обработки персональных данных с использованием средств автоматизации:

- соответствие полномочий пользователя правилам доступа;
- соблюдение пользователями информационных систем персональных данных парольной политики;

- соблюдение пользователями информационных систем персональных данных антивирусной политики;
 - соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных;
 - соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных;
 - соблюдение порядка резервирования баз данных и хранения резервных копий;
 - соблюдение порядка работы со средствами защиты информации;
- Б)Обработки персональных данных без использования средств автоматизации:
- организация хранения бумажных носителей с персональными данными;
 - доступ к бумажным носителям с персональными данными;
 - доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

17.2. Порядок проведения внутренних проверок:

- В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуется проведение периодических проверок условий обработки персональных данных.
- Проверки организуются ответственным за организацию обработки персональных данных или комиссией, назначаемой приказом главного врача Больницы.
- Внутренние проверки проводятся по необходимости в соответствии с указаниями вышестоящего руководства.

17.3. Проверки проводятся непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

17.4. По результатам проверки составляется акт проведения внутренней проверки. Форма акта должна содержать: состав проверяющих, тема проверки, в соответствии с какими требованиями законодательных актов проводится проверка, что проверено, выявлено, какие меры можно предпринять для устранения нарушений, сроки для устранения. Акт подписывается проверяющими.

17.5. Акты хранятся у ответственного за организацию обработки персональных данных. Уничтожение актов проводится ответственным самостоятельно в январе года следующего за проверочным годом, но после полного устранения нарушений.

17.6. О результатах проверки и мерах, необходимых для устранения нарушений, главному врачу докладывает ответственный за организацию обработки персональных данных.

18.ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных работников и пациентов Больницы, установленных действующим законодательством Российской Федерации, настоящим Положением и другими локальными нормативными актами, несут дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.