Приложение № 1
к приказу от 27.01.2023 г. № 34

«Утверждаю»
Главный врач ГБУЗ «Городская поликлиника № 4»
О.Ю. Билко
«__» _____20__г.

Политика
в отношении обработки персональных данных
в ГБУЗ «Городская поликлиника №4»

1. Термины и определения

Для целей настоящей Политики используются следующие понятия:

1.1. *Персональные данные (ПДн)* – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

1.2. *Оператор* – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

1.3. *Обработка ПДн* – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

1.4. *Автоматизированная обработка ПДн* – обработка ПДн с помощью средств вычислительной техники.

1.5. *Распространение ПДн* – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

1.6. *Предоставление ПДн* – действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

1.7. *Блокирование ПДн* – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

1.8. *Уничтожение ПДн* – действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе персональных данных (далее – ИСПДн) и (или) в результате которых уничтожаются материальные носители ПДн.

1.9. *Обезличивание ПДн* – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

1.10. *Информационная система персональных данных* – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

1.11. *Трансграничная передача ПДн* – передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Общие положения

2.1. Настоящая Политика оператора в отношении обработки персональных данных (далее – ПДн) (далее – Политика) разработана в целях выполнения норм федерального законодательства ГБУЗ «Городская поликлиника № 4 г. Петрозаводск» (далее - Оператор).

2.2. Политика характеризуется следующими признаками:

− Разработана в целях обеспечения реализации требований законодательства Российской Федерации в области обработки ПДн субъектов ПДн;

− Раскрывает основные категории ПДн, обрабатываемых Оператором, цели, способы и принципы обработки Оператором ПДн, права и обязанности Оператора при обработке ПДн, права субъектов ПДн, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности ПДн при их обработке;

− Является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке ПДн.

3. Информация об операторе

Наименование: Государственное бюджетное учреждение здравоохранения Республики Карелия «Городская поликлиника N4» г. Петрозаводска.

- Номер: 10-0091112
- Дата и основание внесения в реестр: 17/03/2010 Приказ №147
- ИНН: 1001027310
- Адрес: 185034, Республика Карелия г. Петрозаводск ул. Нойбранденбургская д. 1

4. Правовые основания обработки персональных данных

Политика Оператора в области обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами РФ:

1. Конституцией Российской Федерации.
2. Трудовым кодексом Российской Федерации
3. Гражданским кодексом Российской Федерации.
4. Федеральным законом от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
5. Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».
6. Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
8. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
9. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Во исполнение настоящей Политики Оператором утверждены следующие локальные нормативные правовые акты:

- Приказ о назначении ответственных лиц за обеспечение безопасности персональных данных в информационных системах персональных данных.
- Порядок доступа работников Оператора к сведениям конфиденциального характера.
- Перечень обрабатываемых персональных данных.

- Перечень должностей, работников, допущенных к обработке персональных данных.
- Регламенты взаимодействия с субъектами персональных данных (запросы).
- Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных.
- Акты классификации информационных систем персональных данных.

5. Цель обработки персональных данных

Оператор обрабатывает персональные данные исключительно в следующих целях:
1. Исполнения положений нормативных актов, указанных в п.4 настоящей Политики.
2. Принятие решения о трудоустройстве соискателя.
3. Заключения и выполнения обязательств по трудовым договорам, договорам гражданско-правового характера и договорам с контрагентами.
4. Предоставления субъектам персональных данных квалифицированной медицинской помощи, учета результатов договорных обязательств, а также наиболее полного исполнения учреждением обязательств и компетенций в соответствии с Федеральным законам "Об обязательном медицинском страховании граждан в Российской Федерации" от 29 ноября 2010 года № 326-ФЗ и Федеральным законом "Об основах охраны здоровья граждан в Российской Федерации" от 21.11.2011 № 323-ФЗ.
5. Сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, передача. Обработка персональных данных: смешанная; с передачей по внутренней сети Оператора, без передачи по сети Интернет.

6. Принципы обработки персональных данных

При обработке персональных данных ГБУЗ «ГП №4» придерживается следующих принципов:
1. соблюдение законности получения, обработки, хранения, а так же других действий с персональными данными;
2. обработка персональных данных исключительно с целью исполнения своих обязательств по договору оказания услуг, а также по трудовому договору;
3. сбор только тех персональных данных, которые минимально необходимы для достижения заявленных целей обработки;
4. выполнение мер по обеспечению безопасности персональных данных при их обработке и хранении;
5. соблюдение прав субъекта персональных данных на доступ к его персональным данным;
6. соответствие сроков хранения персональных данных заявленным целям обработки.

7. Обработка персональных данных пациентов Оператора осуществляется для решения следующих задач:

- Обработка амбулаторных карт в электронной форме.
- Формирования отчетов по поликлинике.
- Назначение и начисление счетов на оказание услуг и иных выплат.
- Бухгалтерский учет и контроль финансово-хозяйственной деятельности Оператора и исполнения финансовых обязательств по заключенным договорам.
- Осуществление расчетов с ФОМС и страховыми организациями за оказание медицинских услуг застрахованным лицам.
- Поддержание контактов с законными представителями субъекта персональных данных.
- Проведение лечебно-профилактических мероприятий.
- Иные задачи, необходимые для повышения качества и эффективности деятельности Оператора.

8. Конфиденциальность персональных данных

Работники организации и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

9. Состав персональных данных

В состав обрабатываемых в компании персональных данных пациентов и работников могут входить:

- фамилия, имя, отчество;
- пол;
- дата рождения или возраст;
- паспортные данные;
- адрес проживания;
- номер телефона, факса, адрес электронной почты (по желанию);
- информация о состоянии здоровья;
- другая информация, необходимая для правильного проведения и интерпретации медицинских исследований;
- результаты выполненных медицинских исследований;
- другая информация, необходимая для выполнения обязательств организации в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях, законодательством об обязательных видах страхования, со страховым законодательством.

ГБУЗ «ГП №4» осуществляет обработку данных о состоянии здоровья пациентов в целях оказания медицинских услуг, установления медицинского диагноза при этом обработка персональных данных осуществляется лицами, профессионально занимающимися медицинской деятельностью и обязанными в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

Обработка специальных категорий персональных данных работника, в том числе, сведений о состоянии здоровья, относящихся к вопросу о возможности выполнения работником трудовой функции на основании положений п. 2.3 ч. 2 ст. 10 Закона о персональных данных, в рамках трудового законодательства, в частности согласно ст. 228 ТК РФ, о несчастном случае с работником работодатель обязан проинформировать соответствующие органы.

Обработка специальных категорий персональных данных Работника допускается в случае, если работник организации в письменной форме дал согласие Учреждению на обработку своих специальных категорий персональных данных с целью защиты и реализации своих интересов.

10. Сбор (получение) персональных данных

Персональные данные пациентов организация получает только лично от пациента или от его законного представителя. Персональные данные пациента могут быть получены с его слов и не проверяются.

11. Обработка персональных данных

Обработка персональных данных в организации происходит как неавтоматизированным, так и автоматизированным способом.

К обработке персональных данных в организации допускаются только сотрудники прошедшие определенную процедуру допуска, к которой относятся:

· ознакомление сотрудника с локальными нормативными актами организации (положения, инструкции и т.д.), строго регламентирующими порядок и процедуру работы с персональными данными;
· взятие с сотрудника подписки о соблюдении конфиденциальности в отношении персональных данных при работе с ними.
· получение сотрудником и использование в работе индивидуальных атрибутов доступа к информационным системам компании, содержащим в себе персональные данные. При этом каждому сотруднику выдаются минимально необходимые для исполнения трудовых обязанностей права на доступ в информационные системы.
Сотрудники, имеющие доступ к персональным данным, получают только ту информацию, которая необходима им для выполнения конкретных трудовых функций.

12. Хранение персональных данных

Персональные данные пациентов хранятся в бумажном (амбулаторная карта, бланки направлений, результаты обследований) и электронном виде. В электронном виде персональные данные пациентов хранятся в информационной системе персональных данных организации, а так же в архивных копиях баз данных этих систем. Порядок архивирования и сроки хранения архивных копий баз данных информационной системы персональных данных организации определены в инструкции о резервном копировании, которая является обязательной для исполнения администраторами соответствующей системы.
При хранении персональных данных пациентов и работников соблюдаются организационные и технические меры, обеспечивающие их сохранность и исключающие несанкционированный доступ к ним. К ним относятся:
· назначение сотрудника ответственного за тот или иной способ хранения персональных данных;
· ограничение физического доступа к местам хранения и носителям;
· учет всех информационных систем и электронных носителей, а так же архивных копий.

13. Передача персональных данных третьим лицам

Передача персональных данных третьим лицам возможна в исключительных случаях только с согласия пациента и только с целью исполнения обязанностей перед пациентом в рамках оказания услуг, кроме случаев, когда такая обязанность у организации наступает в результате требований федерального законодательства или при поступлении запроса от уполномоченных государственных органов. В данном случае компания ограничивает передачу персональных данных запрошенным объемом.
Персональные данные пациента (в том числе результаты исследований) могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого пациента, за исключением случаев, когда передача персональных данных без его согласия допускается действующим законодательством РФ. В качестве такого разрешения могут выступать:
· нотариально заверенная доверенность;
· собственноручно написанная клиентом доверенность в присутствии сотрудника ГБУЗ «ГП №4» и им заверенная.

14. Сведения о третьих лицах, участвующих в обработке персональных данных

1. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Оператор в ходе своей деятельности предоставляет персональные данные следующим организациям:
1.1. Федеральной налоговой службе.
1.2. Пенсионному фонду Российской Федерации.

1.3. Фонду медицинского страхования Республики Карелия.
1.4. Страховым медицинским организациям.

15. Меры по обеспечению безопасности персональных данных при их обработке

Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:
1. Назначением ответственных за организацию обработки персональных данных.
2. Осуществлением внутреннего контроля и/или аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам.
3. Ознакомлением работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и (или) обучением указанных сотрудников.
4. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
5. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных.
6. Учетом машинных носителей персональных данных.
7. Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.
8. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
9. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.
10. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.
11. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации. Обязанности должностных лиц, осуществляющих обработку и защиту ПДн, а также их ответственность, определяются в «Положении о персональных данных».

16. Права пациента

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые способы обработки персональных данных;
- сведения о лицах (за исключением работников организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;

- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных своих прав;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению организации, если обработка поручена или будет поручена такому лицу.

Соответствующая информация предоставляется субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его законного представителя. Запрос должен быть составлен в соответствии с требованиями законодательства. Срок реагирования на обращения субъектов персональных данных 10 рабочих дней, с возможностью продления срока предоставления запрашиваемой информации до 5 рабочих дней и направления уведомления об этом в Роскомнадзор.

Настоящая Политика обработки персональных данных действует в отношении всей информации, которую администрация ГБУЗ «ГП №4» может получить о пользователе во время использования им сервисов сайта. Использование сервисов сайта означает безоговорочное согласие пользователя с настоящей Политикой и указанными в ней условиями обработки его персональной информации; в случае несогласия с этими условиями пользователь должен воздержаться от использования сервисов сайта.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017 г.)

При поступлении обращения от субъекта персональных данных о прекращении обработки его персональных данных, обработка персональных данных прекращается в течении 10 дней.

17. **Контроль и надзор за обработкой персональных данных**

1. Ответственный за организацию обработки персональных данных – заместитель главного врача по медицинской части ГБУЗ «Городская поликлиника № 4» Федулова Вероника Юрьевна.
2. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). В случае изменения сведений об обработке персональных данных, необходимо проинформировать Роскомнадзор не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения

18. **Заключительные положения**

1. Настоящая политика утверждается главным врачом.
2. Оператор имеет право вносить изменения в настоящую Политику.
3. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее утверждения и размещения на сайте Оператора, если иное не предусмотрено новой редакцией Политики.