УТВЕРЖДАЮ

Главный врач СПб ГБУЗ
«Городская поликлиника № 93»
_____ Т.И. Исакова
«22» 12 2018 г.

Политика обработки персональных данных в СПб ГБУЗ «Городская поликлиника № 93»

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с пунктом 2 статьи 18.1 Закона № 152-ФЗ от 27 июля 2006 «О персональных данных» и является основополагающим внутренним регулятивным документом СПб ГБУЗ «Городская поликлиника № 93» (далее – Поликлиника), определяющим ключевые направления ее деятельности в области обработки и защиты персональных данных, оператором которых является Поликлиника.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты персональных данных и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в Поликлинике, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите персональных данных, полученных Поликлиникой как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите персональных данных, полученных до ее утверждения.

1.4. Обработка персональных данных в Поликлинике осуществляется в связи с выполнением Поликлиникой функций, предусмотренных ее учредительными документами и определяемых:

– Законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

– Законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Постановлением Правительства РФ от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановлением Правительства РФ от 1 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка персональных данных в Поликлинике осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Поликлиника выступает в качестве работодателя (гл. 14 ТК РФ), в связи с реализацией Поликлиникой своих прав и обязанностей как юридического лица.

1.5. Поликлиника имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее утверждения, если иное не предусмотрено новой редакцией Политики.

2. Термины и принятые сокращения

Персональные данные – любая информация, относящаяся к прямо или косвенно
определенному или определяемому физическому лицу (субъекту персональных данных).

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.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, учреждение, 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.

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.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния.

Медицинская деятельность – профессиональная деятельность по оказанию медицинской
помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях.

Лечащий врач – врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

3. Персональные данные, обрабатываемые Поликлиникой

3.1. Пациенты Поликлиники

Цель обработки: обследование, лечение граждан и осуществление возложенных на Поликлинику законодательством обязанностей.

Состав персональных данных:

Информация, отражающая характер договорных отношений Поликлиники и пациента, включающая ФИО, паспортные данные, адрес регистрации, адрес места жительства, № страхового полиса, контактные данные, характер и перечень существенных условий договора, информация о взаиморасчетах (в случае заключения договора).

Информация медицинского характера, включающая данные о состоянии здоровья (амбулаторная карта, история болезни, история родов), перечень услуг медицинского характера, оказанных пациенту (выполненные анализы и диагностические обследования), перечень назначений, план лечения.

Основания обработки:

- Федеральный закон от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации";
- Закон РФ от 27.11.1992 N 4015-1 "Об организации страхового дела в Российской Федерации".

3.2. Кандидаты на вакантные должности

Цель обработки: подбор персонала.

Состав персональных данных: информация, предоставляемая кандидатом на вакантную должность, включающая ФИО, контактную информацию, образование, опыт работы и другие сведения.

Основания обработки: в целях заключения трудового договора (статья 6 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных").

3.3. Работники и бывшие работники СПБ ГБУЗ «Городская поликлиника № 93».

Цель обработки: осуществление возложенных законодательством обязанностей, выполнение Поликлиникой обязательств, предусмотренных трудовым договором (коллективным договором) между Поликлиникой и работником.

Состав персональных данных:

Сведения о работнике, включая ФИО, паспортные данные, семейное положение, имущественное положение, профессия, год рождения, дата рождения, адрес, социальное положение, образование, доходы, опыт работы и другие сведения, связанные с должностью.

Основания обработки:

- "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ;
- Налоговый кодекс Российской Федерации (часть первая - Федеральный закон от 31.07.1998г. № 146- ФЗ; часть вторая - Федеральный закон от 05.08.2000г. № 117 - ФЗ);
- Постановление Правительства РФ от 24.12.2007г. № 922 "Об особенностях порядка исчисления средней заработной платы";
- Положение по ведению бухгалтерского учета и бухгалтерской отчетности в российской федерации (Приказ Минфина РФ от 29.07.1998 N 34н);
- Трудовой договор между Поликлиникой и работником;
- Регламенты, связанные с воинским учетом, пенсионным обеспечением;
- Письменное согласие работника.

4. Принципы обработки

4.1. Обработка персональных данных производится строго в соответствии со следующими принципами:

- Обработка персональных данных осуществляется на законной и справедливой основе;
- Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей.

4.2. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки, Поликлиника не обрабатывает избыточные персональные данные.

4.3. При обработке персональных данных обеспечивается их точность, достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

4.4. Обрабатываемые персональные данные уничтожаются, либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.5. Получение персональных данных осуществляется следующими способами:

- От родственников или представителей пациента в случае, если они выступают стороной договора на оказание медицинских услуг.
- От субъекта персональных данных лично.
- От страховых компаний, с которыми у пациента заключен договор обязательного или добровольного медицинского страхования.

4.6. Передача персональных данных пациента третьим лицам осуществляется только с письменного согласия субъекта, за исключением следующих случаев:

- данные передаются в целях исполнения договора, одной из сторон которого является субъект персональных данных и в котором явно указано, кому будут переданы указанные персональные данные;
- после обезличивания персональных данных;
- данные передаются в целях обследования и лечения гражданина, не способного из-за своего состояния выразить свою волю;
- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
- по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;
- в случае оказания помощи несовершеннолетнему для информирования его родителей или законного представителя;
- при наличии оснований, позволяющих полагать, что вред здоровью гражданина причинен в результате противоправных действий;
- в целях проведения военно-врачебной экспертизы;
- иных законных основаниях.

Примерами передачи персональных данных пациента служат:

1. Страховые компании:

— передача в страховые компании сведений об оказании медицинских услуг пациентам в рамках страховых программ данной компании (персональные данные, идентифицирующие пациента, перечень услуг медицинского характера, оказанных пациенту, диагноз);

— передача в страховые компании дополнительной медицинской информации о пациенте, связанной с оказанием услуг в рамках страхового случая, являющегося предметом спора (персональные данные, идентифицирующие пациента, извлечение из медицинской карты — перечень назначений, диагноз, план лечения, выполненные анализы и диагностические обследования и т.п) в рамках установленной процедуры разрешения споров. Данная информация предоставляется Поликлиникой уполномоченному персоналу страховой компании, имеющему право работы со сведениями, составляющими врачебную тайну, на ознакомление на бумажных носителях, без права выноса за пределы территории Поликлиники.

2. Лаборатории:

— передача в лаборатории биологического материала для исследования и обезличенного идентификатора, в целях защиты конфиденциальности персональных данных.

5. Принципы обеспечения безопасности персональных данных

5.1. Основной задачей обеспечения безопасности персональных данных при их обработке в Поликлинике является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения персональных данных, разрушения (уничтожения) или искажения их в процессе обработки.

5.2. Для обеспечения безопасности персональных данных Поликлиника руководствуется следующими принципами:

– законность: защита персональных данных основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты персональных данных;

– системность: обработка персональных данных в Поликлинике осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных;

– комплексность: защита персональных данных строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Поликлиники и других имеющихся в Поликлинике систем и средств защиты;

– непрерывность: защита персональных данных обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки персональных данных, в том числе при проведении ремонтных и регламентных работ;

– своевременность: меры, обеспечивающие надлежащий уровень безопасности персональных данных, принимаются до начала их обработки;

– преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты персональных данных осуществляется на основании результатов анализа практики обработки персональных данных в Поликлинике с учетом выявления новых способов и средств реализации угроз безопасности персональных данных, отечественного и зарубежного опыта в сфере защиты информации;

– персональная ответственность: ответственность за обеспечение безопасности персональных данных возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой персональных данных;

– минимизация прав доступа: доступ к персональным данным предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

– гибкость: обеспечение выполнения функций защиты персональных данных при изменении характеристик функционирования информационных систем персональных данных Поликлиники, а также объема и состава обрабатываемых персональных данных;

– специализация и профессионализм: реализация мер по обеспечению безопасности персональных данных осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

– эффективность процедур отбора кадров: кадровая политика Поликлиники предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности персональных данных;

– наблюдаемость и прозрачность: меры по обеспечению безопасности персональных данных должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

– непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля
использования систем обработки и защиты персональных данных, а результаты контроля регулярно анализируются.

5.3. В Поликлинике не производится обработка персональных данных, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки персональных данных в Поликлинике, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Поликлиникой персональные данные уничтожатся или обезличиваются.

5.4. При обработке персональных данных обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Поликлиника принимает необходимые меры по удалению или уточнению неполных или неточных персональных данных.

6. Обработка персональных данных

Получение персональных данных

Все персональные данные следует получать от самого субъекта. Если персональные данные субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных, перечне действий с персональными данными, сроке, в течение которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

Документы, содержащие персональные данные, создаются путем:

а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и т. д.);

б) внесения сведений в учетные формы;

в) получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и т. д.).

Порядок доступа субъекта персональных данных к его персональным данным, обрабатываемым Поликлиникой, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Поликлиники.

Обработка персональных данных

Обработка персональных данных осуществляется:

– с согласия субъекта персональных данных на обработку его персональных данных;

– в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;

– в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц, к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных).

Доступ Работников к обрабатываемым персональным данным осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Поликлиники.

Допущенные к обработке персональных данных Работники под подпись знакомятся с документами Поликлиники, устанавливающими порядок обработки персональных данных, включая документы, устанавливающие права и обязанности конкретных Работников.

Поликлиникой производится устранение выявленных нарушений законодательства об обработке и защите персональных данных.

Цели обработки персональных данных:

– обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с законами от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными постановлением Правительства РФ от 4 октября 2012 г. № 1006;

– осуществление трудовых отношений;

– осуществление гражданско-правовых отношений.

В Поликлинике обрабатываются персональные данные следующих субъектов:

– физических лиц, состоящих с Поликлиникой в трудовых отношениях;

– физических лиц, являющихся близкими родственниками сотрудников Поликлиники;

– физических лиц, уволившихся из Поликлиники;

– физических лиц, являющихся кандидатами на работу;

– физических лиц, состоящих с Поликлиникой в гражданско-правовых отношениях;

– физических лиц, обратившихся в Поликлинику за медицинской помощью.

Персональные данные, обрабатываемые Поликлиникой:

– полученные при осуществлении трудовых отношений;

– полученные для осуществления отбора кандидатов на работу в Поликлинику;

– полученные при осуществлении гражданско-правовых отношений;

– полученные при оказании медицинской помощи.

Полный список персональных данных представлен в перечне персональных данных, утвержденном главным врачом Поликлиники.

Обработка персональных данных ведется:

– с использованием средств автоматизации;

– без использования средств автоматизации.

Хранение персональных данных

Персональные данные субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

Персональные данные, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа (регистратура).

Персональные данные субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

Не допускается хранение и размещение документов, содержащих персональные данные, в открытых электронных каталогах (файлообменниках) в ИСПД.

Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Уничтожение персональных данных

Уничтожение документов (носителей), содержащих персональные данные, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

Уничтожение производится комиссией. Факт уничтожения персональных данных подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

Передача персональных данных

Поликлиника передает персональные данные третьим лицам в следующих случаях:

– субъект выразил свое согласие на такие действия;

– передача предусмотрена законодательством в рамках установленной процедуры.

Перечень третьих лиц, которым передаются персональные данные:

– Пенсионный фонд РФ для учета (на законных основаниях);

– Федеральная налоговая служба РФ (на законных основаниях);

– Фонд социального страхования (на законных основаниях);

– Территориальный фонд обязательного медицинского страхования (на законных основаниях);

– страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);

– кредитные организации (в рамках перечисления заработной платы заработной платы;

– судебные, правоохранительные и надзорные органы в случаях, установленных законодательством;

– бюро кредитных историй (с согласия субъекта);

Защита персональных данных

В соответствии с требованиями нормативных документов Поликлиникой создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту персональных данных.

Основными мерами защиты персональных данных, используемыми Поликлиникой, являются:

- назначение лиц, ответственных за обработку персональных данных, которые осуществляют организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением Поликлиникой и его работниками требований к защите персональных данных;
- определение актуальных угроз безопасности персональных данных при их обработке в ИСПД и разработка мер и мероприятий по защите персональных данных;
- разработка политики в отношении обработки персональных данных;
- установление правил доступа к персональным данным, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в ИСПД;
- установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей персональных данных, обеспечение их сохранности;
- сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;
- сертифицированное программное средство защиты информации от несанкционированного доступа;
- сертифицированные межсетевой экран и средство обнаружения вторжения;

соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности персональных данных;

- установление правил доступа к обрабатываемым персональным данным, обеспечение регистрации и учета действий, совершаемых с персональными данными, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обучение работников Поликлиники, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Поликлиники в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

- осуществление внутреннего контроля и аудита.

7. Основные права субъекта персональных данных и обязанности Поликлиники

Основные права субъекта персональных данных

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных оператором;

– правовые основания и цели обработки персональных данных;

– цели и применяемые оператором способы обработки персональных данных;

– наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту
персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных Законом «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

– иные сведения, предусмотренные Законом «О персональных данных» или другими федеральными законами.

Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Обязанности Поликлиники

Поликлиника обязана:

– при сборе персональных данных предоставить информацию об обработке его персональных данных;

– в случаях, если персональные данные были получены не от субъекта персональных данных, уведомить субъекта;

– при отказе в предоставлении персональных данных субъекту разъясняются последствия такого отказа;

– опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;

– принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования,

предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

– давать ответы на запросы и обращения субъектов персональных данных, их представителей и уполномоченного органа по защите прав субъектов персональных данных.