«УТВЕРЖДАЮ»
Главный врач
С.В. Попов
«03» февраля 2020 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных СПб ГБУЗ Клиническая больница Святителя Луки

I. Общие положения

1.1 Настоящее Положение об обработке и защите персональных данных (далее - Положение) определяет политику, порядок и условия обработки персональных данных и меры по обеспечению безопасности персональных данных в СПб ГБУЗ Клиническая больница Святителя Луки (далее - Учреждение), устанавливает процедуры, направленные на предотвращение нарушений законодательства Российской Федерации в сфере, связанной с обработкой персональных данных.

1.2 Цель настоящего Положения – обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных работников, пациентов, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных в СПб ГБУЗ Клиническая больница Святителя Луки (далее - Оператор).

1.3 Все вопросы, связанные с обработкой персональных данных, не урегулированные настоящим Положением, разрешаются в соответствии с действующим законодательством Российской Федерации в области персональных данных.

1.4 Настоящее Положение разработано с учётом принципов, правил и требований, установленных основными правовыми нормативными актами, регламентирующими требования к процессам обработки персональных данных, соблюдения конфиденциальности, в том числе в медицинских организациях:

- Конституция Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Кодекс Российской Федерации об административных правонарушениях ;
-Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» № 188 от 06.03.1997 г.;
- Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
-Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

- Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

- Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

- Федеральный закон от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств»;

- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»);

- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

- Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена ФСТЭК 15.02.2008);

- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения;

- ГОСТ 34.603-92 Виды испытаний автоматизированных систем.;

- Модель угроз типовой медицинской информационной системы типового лечебно-профилактического учреждения (Минздравсоцразвития России, ноябрь 2009; согласована с ФСТЭК, письмо от 27.11.2009 № 240/2/4009 за подписью заместителя директора ФСТЭК А.Гапонова);

- Методические рекомендации по организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости (Минздравсоцразвития России, утверждены 23.12.2009 директором Департамента информатизации Минздравсоцразвития России О.В.Симаковым, согласованы 22.12.2009 начальником 2-го управления ФСТЭК России А.В.Куц);

- Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений и организаций здравоохранения, социальной сферы, труда и занятости (Минздравсоцразвития России, утверждены 23.12.2009 директором Департамента информатизации Минздравсоцразвития России О.В.Симаковым, согласованы 22.12.2009 начальником 2-го управления ФСТЭК России А.В.Куц).

- Иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.

1.5 Настоящее Положение обязательно для всех работников Учреждения, получающих доступ к сведениям, составляющим персональные данные, врачебную и коммерческую тайну.

1.6 Режим конфиденциальности в отношении персональных данных снимается:

– в случае их обезличивания;

– по истечении срока их хранения;

– в других случаях, предусмотренных федеральными законами РФ.

II. Основные понятия и определения.

2.1. Для целей настоящего Положения используются следующие основные понятия и определения:

– «персональные данные» - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

– «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;

– «субъект» - субъект 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;

- «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»- информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

– «конфиденциальность персональных данных»- обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

– «конфиденциальная информация» - это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством РФ;

– «трансграничная передача персональных данных» - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

--«общедоступные источники персональных данных» - общедоступные источники персональных данных (в том числе справочники, адресные книги), в которые с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год

и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных;
– «информация» - сведения (сообщения, данные) независимо от формы их представления;
– «доступ к информации» - возможность получения информации и ее использования;
– «документированная информация» - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
– «врачебная тайна» - это сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении;
– «персональные данные пациента» - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу;
– «неуполномоченное лицо» - лицо, не имеющее права законного допуска к персональным данным.

III. Состав персональных данных субъектов персональных данных

3.1 Персональным данные работника СПб ГБУЗ Клиническая больница Святителя Луки включают в себя:

фамилию, имя, отчество; дату и место рождения; паспортные данные; семейное положение; доходы, включающие, например, заработную плату, премиальные выплаты; место жительства; контактную информацию работника и членов его семьи, включающую, например, номер сотового телефона, номер домашнего телефона, адрес электронной почты; информацию о состоянии здоровья, которая обязательно должна быть сообщена работником при приеме на работу согласно законодательству РФ; индивидуальный номер налогоплательщика; номер страхового свидетельства государственного пенсионного страхования; информацию из военного билета; информацию об образовании; номер банковского счета; биометрические персональные данные в виде фотоизображения; иную информацию в предусмотренных законодательством РФ случаях.

3.2. Персональным данные пациента СПб ГБУЗ Клиническая больница Святителя Луки включают в себя:

фамилия, имя, отчество, год, месяц, дата и место рождения, серия и номер паспорта, адрес регистрации и фактического проживания, идентификационный номер налогоплательщика (ИНН), страховое свидетельство государственного пенсионного страхования (СНИЛС), семейное, социальное, образование, профессия, должность, специальность, серия и номер страхового медицинского полиса ДМС и его действительность, номер амбулаторной карты, сведения о состоянии здоровья, в том числе группа здоровья, группа инвалидности степень ограничения к трудовой деятельности, зарегистрированные диагнозы по результатам обращения пациентов к врачу, информация об оказанных медицинских услугах, в том числе о проведенных лабораторных анализах и исследованиях и их результатах, выполненных оперативных вмешательствах, случаях стационарного лечения их результатах, о выданных листах временной нетрудоспособности с указанием номера листа нетрудоспособности и периода нетрудоспособности, информация о выписанных и отпущенных лекарственных средствах и изделиях медицинского назначения. В отдельных случаях с учетом специфики обследования, согласно действующего законодательства РФ, Оператор может предусматривать необходимость предъявления дополнительных документов.

IV. Общие принципы обработки персональных данных

4.1. Обработка персональных данных осуществляется на законной и справедливой основе.
4.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
4.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
4.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
4.5. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям их обработки.
4.6. При обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор принимает все необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

V. Конфиденциальность персональных данных

5.1 Операторы, 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.

VI. Обязанности работников Учреждения

6.1 Работники Учреждения, получившие доступ к персональным данным и врачебной тайне субъектов в связи с исполнением трудовых обязанностей, обязуются обеспечивать конфиденциальность и сохранность таких сведений. Работники при поступлении на работу в Учреждение должны быть ознакомлены отделом кадров под роспись с настоящим Положением.

6.2 Обеспечивая конфиденциальность, работник обязуется:

– знать и соблюдать требования по получению, обработке, передаче, хранению, получению сведений, составляющих профессиональную тайну и персональные данные работников, пациентов, предусмотренные нормативными правовыми актами, коллективным договором, соглашениями, должностной инструкцией, локальными нормативными актами Учреждения, трудовым договором;

– принимать меры по установлению и сохранению режима конфиденциальности, предусмотренные нормативными правовыми актами, локальными нормативными актами Учреждения, трудовым договором;

– не использовать без разрешения обладателя или субъекта персональных данных информацию ограниченного доступа в целях, не связанных с осуществлением трудовой функции;

– не разглашать сведения, составляющие врачебную тайну и персональные данные пациентов, а также не совершать иных деяний, влекущих уничтожение или утрату таких

сведений (их материальных носителей) или потерю ее коммерческой или иной ценности для ее обладателя;

– незамедлительно сообщать об утрате или несанкционированном уничтожении сведений, составляющих врачебную тайну и персональные данные, своему непосредственному руководителю, а также об иных обстоятельствах, создающих угрозу сохранения конфиденциальности таких сведений (в том числе о попытках неправомерного доступа к информации со стороны неуполномоченных лиц);

– обеспечить хранение первичной учетной документации по учету труда и его оплаты, к которой, в частности, относятся документы по учету кадров, документы по учету использования рабочего времени и расчетов с работниками по оплате труда, медицинская документация и др. При этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные;

6.3 При прекращении трудовых отношений с Учреждением работник обязан сдать все материальные носители сведений, содержащие врачебную тайну и персональные данные субъектов, а также ключи от помещений и шкафов, в которых они хранятся.

6.4 Сотрудники отдела информационных технологий обеспечивают следующие меры по защите хранящейся на сервере информации:

– ограничение сетевого доступа на сервер, для определенных пользователей;

– организацию в отдельном сегменте сети всех компьютеров пользователей и серверов с ограниченным доступом;

– организацию контроля технического состояния серверов и уровней защиты и восстановления информации;

– проведение регулярного резервного копирования информации;

– ведение аудита действий пользователей и своевременное обнаружение фактов несанкционированного доступа к информации.

VII. Защита персональных данных субъектов

7.1 Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает 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.

7.2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) 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, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) 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;
9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

VIII. Требования по получению, обработке, хранению и использованию информации ограниченного доступа и условия обработки персональных данных

8.1 Персональные данные субъектов персональных данных могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.
8.2 Информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных, в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства. Сбор и обработка персональных данных осуществляется исключительно с письменного согласия субъекта. Требования при обработке персональных данных работника установлены ст. 86 Трудового кодекса РФ/

8.3 Обработка персональных данных пациента осуществляется с согласия субъекта персональных данных на обработку его персональных данных и может осуществляться исключительно в целях ведения медицинского учета, в целях установления медицинского диагноза и оказания медицинской помощи, в целях оформления и исполнения договорных обязательств с пациентом в соответствии с требованиями законодательства Российской Федерации в области персональных данных.
8.4 Обработка персональных данных субъекта может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, количества и качества выполняемой работы, обследования, наблюдения и лечения пациентов и обеспечения сохранности имущества оператора, работника, пациента, и третьих лиц.
8.5 Обработка персональных данных пациентов может осуществляться для статистических или иных научных целей при условии обязательного обезличивания персональных данных.
8.6 В случае выявления неправомерной обработки персональных данных при обращении пациента или его представителя либо по запросу пациента или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении пациента или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или

получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы пациента или третьих лиц.

8.7 В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных пациентом или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

8.8 В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить пациента или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

8.9 В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является пациент, иным соглашением между оператором и пациентом либо если оператор не вправе осуществлять обработку персональных данных без согласия пациента, на основаниях, предусмотренных Федеральным законом №152-ФЗ «О персональных данных» или другими федеральными законами.

8.10 В случае отзыва пациентом согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и пациентом либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом №152-ФЗ или другими федеральными законами.

8.11 В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение

персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

8.12 Информация о персональных данных субъекта предоставляется оператору субъектом устно, либо путем заполнения личных карточек формы Т-2 для работников, которые хранятся в личном деле в архиве. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом и от него должно быть получено письменное согласие (либо письменный отказ). В письменном уведомлении оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных (например, оформление запроса в медицинское организация о прохождении обследования и лечения и т.п.) и последствиях отказа субъекта дать письменное согласие на их получение.

8.13 Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом №152-ФЗ «О персональных данных». В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии с Федеральным законом №152-ФЗ «О персональных данных».

8.14 В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

8.15 Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

8.16 Оператор обязан рассмотреть возражение в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

8.17 Оператор не имеет права получать и обрабатывать персональные данные субъекта, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия

8.18 Оператор не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами РФ.

8.19 При поступлении на работу работник представляет следующие документы, содержащие персональные данные о себе:

– паспорт или иной документ, удостоверяющий личность;
– трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
– страховое свидетельство государственного пенсионного страхования;
– свидетельство о регистрации индивидуального налогового номера (ИНН);
– документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
– документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки.

При оформлении работника ответственным работником отдела кадров заполняется унифицированная форма Т-2 "Личная карточка работника", в которой отражаются следующие анкетные и биографические данные работника:
– общие сведения (Ф.И.О., дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
– сведения о воинском учете;
– данные о приеме на работу;
– сведения об аттестации;
– сведения о повышенной квалификации;
– сведения о профессиональной переподготовке;
– сведения о наградах (поощрениях), почетных званиях; – сведения об отпусках; – сведения о социальных гарантиях; – сведения о месте жительства и о контактных телефонах.
8.20 При приеме к врачу пациент представляет следующие документы, содержащие персональные данные о себе:
– паспорт или иной документ, удостоверяющий личность, гражданство;
– полис ОМС;
– страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС);
– в отдельных случаях с учетом специфики обследования в Учреждении действующим законодательством РФ может предусматриваться необходимость предъявления дополнительных документов.

Запрещается требовать от субъекта персональных данных документы помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

8.21 При заключении трудового договора и в ходе трудовой деятельности может возникнуть необходимость в предоставлении служащим документов:

– о возрасте детей;
– об инвалидности;
– о донорстве;
– о составе семьи;
– о необходимости ухода за больным членом семьи;
– прочие.
8.22 После того, как будет принято решение о приеме работника на работу, а также впоследствии в процессе трудовой деятельности, к документам, содержащим персональные данные субъекта, также будут относиться:

– трудовой договор;
– приказ о приеме на работу;
– приказы о поощрениях и взысканиях;
– медицинский осмотр сотрудника при приеме на работу (флюорография грудной клетки, анализ крови на RW, ВИЧ, гепатиты и т.д.);
– приказы, связанные с прохождением учебы сотрудников;
– карточка унифицированной формы Т-2, утвержденная постановлением Госкомстата России от 05.01.04 №1;
– другие документы согласно законодательству Российской Федерации
8.23 В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ возможно получение и обработка данных о частной жизни работника только с его письменного согласия.
8.24 При принятии решений относительно работника на основании его персональных данных не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.
8.25 Обработка и хранение сведений, составляющих врачебную тайну и персональные данные пациентов, осуществляется в таком порядке и таким способом, которые исключают возможность доступа к ней неуполномоченных лиц.
8.26 Обработка персональных данных пациентов осуществляется с их согласия, за исключением обработки персональных данных, осуществляемой:
– в статистических или иных научных целях в отношении обезличенных персональных данных пациента;
– в иных случаях, установленных федеральным законом.
8.27 В целях обеспечения достоверности персональных данных субъект обязан:

- При приеме на работу, визите к врачу предоставить оператору полные достоверные данные о себе.
- В случае изменения сведений, составляющих персональные данные, работник незамедлительно должен предоставить данную информацию в отдел кадров Учреждения.
8.28 Не допускается сообщение диагноза заболевания, его прогноза и лечения и др. персональных данных пациента не уполномоченным лицам. Сообщение указанной информации в доступной форме возможно только самому пациенту, а также его законным представителям в предусмотренных законом случаях.
8.29 В других случаях передача сведений, составляющих врачебную тайну и персональные данные пациента другим лицам допускается только с согласия пациента или его законного представителя в интересах обследования и лечения пациента, для проведения научных исследований, публикации в научной литературе, использования этих сведений в учебном процессе и в иных целях.
8.30 При отсутствии согласия субъекта обработка общих категорий персональных данных допускается в случае, если:
– осуществляется на основании и во исполнение федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
– обработка персональных данных осуществляется в статистических или иных научных целях при условии обязательного обезличивания персональных данных;
8.31 Обработка персональных данных осуществляется:
– без использования средств автоматизации;
– с использованием медицинской информационной системы;
8.32 Предоставление сведений, составляющих врачебную тайну, без согласия пациента или его законного представителя иным лицам допускается:

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю, с учетом положений пункта 1 части 9 статьи 20 Федеральный закон от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации";
2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
3) 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;
3.1) в целях осуществления уполномоченными федеральными органами исполнительной власти контроля за исполнением лицами, признанными больными наркоманией либо потребляющими наркотические средства или психотропные вещества без назначения врача либо новые потенциально опасные психоактивные вещества, возложенной на них при назначении административного наказания судом обязанности пройти лечение от наркомании, диагностику, профилактические мероприятия и (или) медицинскую реабилитацию;
4) в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;
5) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти и федеральных государственных органов, в которых федеральным законом предусмотрена военная и приравненная к ней служба;
6) в целях расследования несчастного случая на производстве и профессионального заболевания, а также несчастного случая с обучающимся во время пребывания в организации, осуществляющей образовательную деятельность, и в соответствии с частью 6 статьи 34.1 Федерального закона от 4 декабря 2007 года N 329-ФЗ "О физической культуре и спорте в Российской Федерации" несчастного случая с лицом, проходящим спортивную подготовку и не состоящим в трудовых отношениях с физкультурно-спортивной организацией, не осуществляющей спортивной подготовки и являющейся заказчиком услуг по спортивной подготовке, во время прохождения таким лицом спортивной подготовки в организации, осуществляющей спортивную подготовку, в том числе во время его участия в спортивных соревнованиях, предусмотренных реализуемыми программами спортивной подготовки;
7) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;
8) в целях осуществления учета и контроля в системе обязательного социального страхования;
9) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с Федеральный закон от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

8.33 При передаче персональных данных пациентов третьим лицам должны быть соблюдены следующие требования:
– персональные данные предоставляются только с письменного согласия пациента, за исключением случаев, предусмотренных федеральным законом;

– предупреждение лиц, получивших доступ к персональным данным пациента о возможности использования сведений только в установленных целях и об ответственности за нарушение законодательства в этой сфере;
– соблюдение режима конфиденциальности получателями.

8.34 Не допускается передача и выдача документов, содержащих врачебную тайну и персональные данные пациента неуполномоченным лицам. Передача соответствующих документов в регистратуру возможна только самим лечащим врачом или медицинским персоналом, имеющим допуск к такой информации.

8.35 При регистрации пациента и выдачи ему медицинской карты и иных документов, касающихся состояния его здоровья, также должна обеспечиваться конфиденциальность.

9.1 Хранение сведений, составляющих медицинскую тайну и персональные данные пациентов осуществляется в порядке, исключающем их утрату, неправомерное использование или получение доступа неуполномоченными лицами, только в соответствии с целями, определившими их получение.

9.2 Медицинские карты пациентов подлежат сдаче в регистратуру и архив, для их последующего хранения. Не допускается доступ в помещение для хранения неуполномоченных лиц.

9.3 Персональные данные субъектов хранятся на бумажных носителях в помещении регистратуры. Для этого используются специально оборудованные шкафы и сейфы.

9.4 Конкретные обязанности по ведению, хранению личных дел субъектов, заполнению, хранению и выдаче трудовых книжек, иных документов, отражающих персональные данные субъектов, возлагается на ответственное лицо отдела кадров.

9.5 Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

9.6 Сведения о субъектах персональных данных Учреждения хранятся также на электронных носителях – в базах данных МИС, 1С: «Зарплата + Кадры»; Осуществляется передача информации по внутренней сети и сети Интернет; операции с персональными данными: сбор, хранение, накопление, уточнение, передача, уничтожение данных.

9.7 При получении сведений, составляющих персональные данные субъектов, заинтересованные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций и заданий.

9.8 Все медицинские документы, результаты анализов должны храниться в шкафах, оборудованных замками.

9.9 Использование сведений, составляющих врачебную тайну или персональные данные пациентов, допускается только в целях обследования и лечения пациентов в Учреждении.

9.10 Не допускается использовать информацию о пациентах за пределами рабочего времени и (или) в целях, не связанных с осуществлением своих трудовых обязанностей Учреждении, а также после прекращения трудовых отношений с Учреждением.

9.11 Вынос резервных и технологических копий баз данных МИС, содержащих информацию персонального характера, врачебную тайну, из Учреждения запрещен. Передача и копирование резервных и технологических копий баз данных допустима только для прямого использования с целью технологической поддержки МИС.

9.12 Копировать и делать выписки персональных данных работника разрешается исключительно в служебных целях с письменного разрешения руководителя или уполномоченного им лица.

9.13 Хранение резервных и технологических копий баз данных МИС, содержащих информацию персонального характера, осуществляется на серверах организации и сменных носителях, доступ к которым ограничен.

9.14 При принятии решений, затрагивающего интересы субъекта персональных данных, нельзя основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

9.15 Защита персональных данных работников и пациента от неправомерного их использования или утраты обспечивается Учреждением за счет своих средств, в порядке, установленном федеральным законодательством и другими нормативными документами.

X. Права и обязанности субъектов персональных данных в целях защиты персональных данных

10.1 Для своевременной и полной реализации своих прав, субъект обязан предоставить организации-оператору достоверные персональные данные.

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

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) 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;

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

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

10.2 Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

10.2.1 обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

10.2.2 обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

10.2.3 доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

XI. Порядок передачи персональных данных субъектов

11.1. Внутренний доступ (доступ внутри Учреждения).

11.2. Право доступа к персональным данным работника имеют:
- Главный врач;
- Заместители главного врача;
- Главный бухгалтер;
- Работники отдела кадров;
- Работники экономического отдела;
- Работники бухгалтерии;
- Работники отдела информационных технологий - к тем данным, которые необходимы для выполнения конкретных функций;
- Операторы ЭВМ - к тем данным, которые необходимы для выполнения конкретных функций;
- Главная медицинская сестра;
- Работники канцелярии - - к тем данным, которые необходимы для выполнения конкретных функций;
- Руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников подразделения);
- Специалист по охране труда - к тем данным, которые необходимы для выполнения конкретных функций;
- Юрисконсульт - к тем данным, которые необходимы для выполнения конкретных функций;
- Секретарь - к тем данным, которые необходимы для выполнения конкретных функций;
- сам работник, носитель данных.

11.3. Доступ к персональным данным пациентов имеют следующие должностные лица Учреждения, непосредственно использующие их в рамках выполнения своих должностных обязанностей:
-Главный врач;
- Заместители главного врача;
- Главный бухгалтер;
- Работники бухгалтерии;
- Работники отдела организации внебюджетной деятельности;
- Работники отдела информационных технологий, операторы ЭВМ;
- Работники организационно-методического отдела;
- Работники экономического отдела, непосредственно обрабатывающие персональные данные пациентов;
- Работники бухгалтерии;
- Юрисконсульт - к тем данным, которые необходимы для выполнения конкретных функций;
- Работники канцелярии - к тем данным, которые необходимы для выполнения конкретных функций;
- Архивариус - к тем данным, которые необходимы для выполнения конкретных функций;
- Секретарь - к тем данным, которые необходимы для выполнения конкретных функций;
- Врачебный персонал (заведующие отделениями, врачи);
-Средний медицинский персонал, в т. ч. медицинские регистраторы.

11.4 Доступ к МИС Учреждения разграничен политикой безопасности системы, реализуемой с использованием технических и организационных мероприятий.

11.5 Каждый пользователь имеет индивидуальную учетную запись, которая определяет его права и полномочия в МИС. Информация об учетной записи не может быть передана другим лицам. Пользователь несет персональную ответственность за конфиденциальность сведений собственной учетной записи.

11.6 Запрещается использование для доступа к МИС Учреждения учетных записей других пользователей.

11.7 Созданием, удалением и изменением учетных записей пользователей МИС занимаются уполномоченные администраторы в соответствии с должностными обязанностями.

11.8 При передаче персональных данных субъектов работники Учреждения, имеющие доступ к персональным данным, должны соблюдать следующие требования:

11.8.1 Не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных Трудовым кодексом РФ или иными федеральными законами. Учитывая, что Трудовой кодекс РФ не определяет критерии ситуаций, представляющих угрозу жизни или здоровью субъекта, оператор в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы. Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных субъекта, либо отсутствует письменное согласие субъекта на предоставление его персональных сведений, либо, по мнению оператора, отсутствует угроза жизни или здоровью субъекта, оператор обязан отказать в предоставлении персональных данных лицу.

11.8.2 Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

11.8.3 Предупредить лиц, получающих персональные данные субъекта, 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.

11.8.4 Передавать персональные данные работника представителю работника в порядке, установленном Трудовым кодексом РФ и настоящим Положением, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанным представителем его функций.

XII. Организация конфиденциального делопроизводства

12.1 Все документы, содержащие информацию ограниченного доступа, должны сохраняться в режиме конфиденциальности и быть доступными только тем лицам, которые имеют допуск к таким сведениям в силу исполнения ими своих должностных обязанностей. Организация конфиденциального делопроизводства должна исключать ознакомление с информацией иных лиц, не имеющих такого доступа.

12.2 На документах конфиденциального характера в правом верхнем углу первого листа ставится гриф «Конфиденциально» с указанием номера экземпляра. На обороте листа (обложки) документа с грифом «Конфиденциально» указываются Список лиц, которые вправе использовать документ при осуществлении своей трудовой функции

12.3 Приказом по Учреждению назначается группа лиц, ответственных за учет, хранение и использование информации, ограниченного доступа.

12.4 Документы и иные материальные носители, содержащие конфиденциальную информацию, хранятся в сейфе или ином закрытом помещении, приспособлении, к которому отсутствует свободный доступ других лиц.

12.5 Движение документов с грифом «Конфиденциально» должно своевременно отражаться в «Журнале учета движения конфиденциальных документов».

12.6 При работе с документами, имеющими гриф «Конфиденциально» запрещено:

– делать выписки в целях, не связанных с оказанием медицинской помощи пациенту или не связанных с осуществлением трудовой функции;

– знакомить с такими документами, в том числе в электронном виде других лиц, не имеющих соответствующего доступа;

– использовать информацию из таких документов в открытых сообщениях, докладах, переписке, рекламных изданиях (такое использование допускается только при условии обезличивания информации;

– оставлять на рабочем месте документы и иные носители информации с грифом «Конфиденциально»;

– не допускать к компьютерам, содержащим персональные данные пациентов и врачебную тайну, посторонних лиц;

– не оставлять включенными компьютеры, содержащие персональные данные субъектов.

XIII. Особенности предоставления доступа к персональным данным

13.1 При передаче конфиденциальных данных должны соблюдаться следующие требования:

13.2 Не сообщать данные третьей стороне без письменного согласия соответствующего лица, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных федеральным законом.

13.3 Не сообщать данные в коммерческих целях без его письменного согласия другой стороне.

Предупредить лиц, получивших конфиденциальную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие данные, обязаны соблюдать режим конфиденциальности. Осуществлять передачу конфиденциальных данных в пределах Учреждения в соответствии с настоящим Положением.

13.4 Разрешать доступ к конфиденциальной информации только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те данные, которые необходимы для выполнения конкретной функции.

13.5 Передавать персональные данные работников, пациентов их законным, полномочным представителям в порядке, установленном законодательством РФ, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции. Конфиденциальную информацию по Договорам передавать третьим лицам согласно условиям Договора.

13.6 Внешний доступ

13.6.1 К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

– налоговые инспекции; правоохранительные органы;

– органы статистики;

– страховые агентства;

– военкоматы;

– органы социального страхования;

– ТФОМС,

- СМО, СМК

– пенсионные фонды;

– подразделения муниципальных органов управления;

– органы исполнительной власти.

13.6.2 Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

13.6.3 Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.
13.6.4 Другие организации. Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

XIV. Ответственность за нарушение норм, регулирующих обработку и защиту конфиденциальной информации

14.1 К видам нарушения режима конфиденциальности относятся:
– разглашение информации, составляющей врачебную тайну, персональные данные работников, пациентов;
– неправомерное использование информации, составляющей конфиденциальную информацию (использование без согласия субъекта и (или) в целях, не связанных с оказанием медицинской помощи пациенту в Учреждении;
– утрата документов и иных материальных носителей сведений, составляющих конфиденциальную информацию в соответствии с разделом настоящего положения;
– неправомерное уничтожение документов, содержащих конфиденциальную информацию;
– нарушение требования хранения документов, содержащих конфиденциальную информацию (хранение в открытом доступе, оставление на рабочем столе и т.д.);
– передача документов и сведений, составляющих конфиденциальную информацию неуполномоченным лицам;
– другие нарушения требований законодательства РФ и настоящего Положения.
14.2 Нарушение требований законодательства о персональных данных влечет наступление уголовной, административной, дисциплинарной, гражданско-правовой ответственности.
14.3 Разглашение конфиденциальной информации может являться основанием для расторжения трудового договора с работниками Учреждения по подпункту «в» пункта 6 части первой статьи 81 Трудового кодекса Российской Федерации. Работники Учреждения, виновные в нарушении порядка обращения с конфиденциальной информацией, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами. Неоднократное нарушение требований режима конфиденциальности может послужить основанием для прекращения трудового договора по пункту 5 части первой статьи 81 Трудового кодекса Российской Федерации.
14.4 Контроль исполнения требований настоящего Положения осуществляется ответственным за обеспечение безопасности персональных данных.
14.5 Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несет персональную ответственность за данное разрешение.

XV. Заключительные положения

15.1 Настоящее Положение вступает в силу с момента его утверждения Главным врачом СПб ГБУЗ Клиническая больница Святителя Луки и действует до утверждения нового Положения .
15.2 Пациенты Учреждения, а также их законные представители, имеют право, ознакомиться с настоящим Положением.

15.3 Работники Учреждения подлежат ознакомлению с данным Положением в порядке, предусмотренном приказом главного врача Учреждения под личную подпись.

15.4 В обязанности работников, осуществляющих первичный сбор персональных данных пациента, входит получение согласия пациента на обработку его персональных данных под личную подпись.

15.5 В обязанности работодателя входит ознакомление всех работников с настоящим Положением и лиц, принимаемых на работу, до подписания трудового договора, под личную подпись.