



УТВЕРЖДАЮ

Главный врач

ГБУЗ «Ленинская ЦРБ»

Д.А. Крайнов

«29» сентября 2022 г.

**ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
государственного бюджетного учреждения здравоохранения «Ленинская центральная
районная больница» в отношении обработки и защиты персональных данных**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности государственного бюджетного учреждения здравоохранения «Ленинская центральная районная больница» (далее – Политика) разработана в соответствии с Федеральным законом Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных» (далее - Федеральный закон), постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее - ПП №1119), постановлением Правительства Российской Федерации от 21.03.2012 №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ними нормативными правовыми актами, операторами являющимися государственными или муниципальными органами» (далее - ПП №211) и устанавливает единый порядок обработки персональных данных в ГБУЗ «Ленинская ЦРБ»

1.2. В Политике используются следующие термины и понятия:

— *персональные данные* - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

— *обработка персональных данных* - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение 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;

— *обработка персональных данных без использования средств автоматизации (неавтоматизированная)* - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.3. Правовым основанием обработки персональных данных в государственном учреждении здравоохранения «Ленинская центральная районная больница» (далее – ГБУЗ «Ленинская ЦРБ») являются:

— Трудовой кодекс РФ;

— Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

— Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

— Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных

технологиях и о защите информации»;

— постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

— договорные отношения между ГБУЗ «Ленинская ЦРБ» и работниками ГБУЗ «Ленинская ЦРБ».

1.4. Обработка персональных данных (далее - ПДн) осуществляется с целью выполнения нормативных правовых актов и соблюдения законодательства РФ (трудового, налогового, пенсионного, страхового, архивного, бухгалтерского и др.), ведения кадровой работы в ГБУЗ «Ленинская ЦРБ», содействия работников в трудоустройстве, обучении и продвижении по службе, обеспечения контроля количества и качества выполняемой работы, а также с целью исполнения договорных отношений.

1.5. При обработке ПДн работников ГБУЗ «Ленинская ЦРБ» осуществляются следующие действия с персональными данными: сбор, запись, систематизация, накопление, хранение, обновление (изменение), извлечение, использование (печать), распространение (передача), удаление, уничтожение.

1.6. В ИСПДн ГБУЗ «Ленинская ЦРБ» защите подлежат персональные данные работников и пациентов ГБУЗ «Ленинская ЦРБ».

1.7. К персональным данным работников, обрабатываемым и защищаемым в ИСПДн ГБУЗ «Ленинская ЦРБ», относятся следующие сведения:

- фамилия, имя, отчество;
- дата и место рождения;
- адрес регистрации (прописки);
- адрес фактического проживания;
- сведения о гражданстве;
- паспортные данные;
- сведения об образовании, квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);
- сведения о профессиональной (трудовой) деятельности;
- подразделение, должность, режим работы;
- вид МП, условие МП, тип занятости должности;
- номер страхового свидетельства государственного пенсионного страхования (СНИЛС);
- номер домашнего или личного телефона;
- сведения о воинском учете (для военнообязанных лиц и лиц, подлежащих призыву на военную службу);
- сведения о наградах, поощрениях, почетных званиях, социальных льготах;
- сведения о заработной плате;
- сведения о составе семьи;
- стаж работы;
- сведения о трудовом договоре, должности, а также номер расчетного счета;
- иные сведения о работнике, нахождение которых в личном деле работника необходимо для корректного документального оформления трудовых правоотношений с работником.

1.8. К персональным данным пациентов, обрабатываемым и защищаемым в ИСПДн ГБУЗ «Ленинская ЦРБ», относятся следующие сведения:

- фамилия, имя, отчество;
- дата и место рождения;
- адрес регистрации (прописки);
- адрес фактического проживания;
- паспортные данные;
- номер страхового медицинского полиса;
- данные о состоянии здоровья.

2. ОСНОВНЫЕ УСЛОВИЯ ПРОВЕДЕНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка ПДн в ГБУЗ «Ленинская ЦРБ» осуществляется путем смешанной обработки (как автоматизированной, так и неавтоматизированной) с передачей по внутренней локальной сети, и нарочным способом в уполномоченные органы и по сетям связи общего пользования и (или) сетям международного информационного обмена.

2.2. Трансграничная передача персональных данных не осуществляется.

2.3. В ГБУЗ «Ленинская ЦРБ» предпринимаются необходимые организационные и технические меры по защите персональных данных. Целью защиты ПДн является обеспечение их конфиденциальности.

2.4. Принимаемые меры основаны на требованиях статей 18.1 и 19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и иных нормативных актов.

К таким мерам в частности относятся:

- назначение лиц ответственных за организацию обработки и защиты персональных данных;
- учет лиц, допущенных к работе с персональными данными;
- разработка и ввод в действие Политика информационной безопасности государственного бюджетного учреждения здравоохранения «Ленинская центральная районная больница», «Положение по обработке и защите персональных данных в государственном учреждении здравоохранения «Ленинская центральная районная больница» и других внутренних организационно-распорядительных документов по обеспечению безопасности персональных данных;
- оформление перечня ПДн, подлежащих защите в ГБУЗ «Ленинская ЦРБ»;
- определение уровня защищенности ИСПДн в целях реализации дифференциального подхода к обеспечению безопасности ПДн и оптимизации расходов на создание и эксплуатацию системы защиты ПДн;
- разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИС. Система защиты ПДн описывается во внутренних организационно-распорядительных документах;
- установка и ввод в эксплуатацию средств защиты информации в соответствии с требованиями нормативно-методических документов, эксплуатационной и технической документацией;
- проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- поэкземплярный учет применяемых средств защиты информации, в том числе СКЗИ, эксплуатационной и технической документации к ним;
- хранение документации и носителей ПДн осуществляется в специально предназначенных для этого местах (сейфах, шкафах и пр.);
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обучение лиц, эксплуатирующих применяемые в ИСПДн средства защиты информации, правилам работы с ними;
- организация режима обеспечения безопасности помещений, в которых производится обработка персональных данных;
- постоянный контроль за обеспечением уровня защищенности персональных данных;
- контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным. Разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования СЗИ, которые могут привести к нарушению

конфиденциальности ПДн, или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

- восстановление персональных данных, модифицированных или уничтоженных вследствие доступа к ним;
- осуществление контроля за применяемыми мерами по обеспечению безопасности персональных данных.

3. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1. Обработка персональных данных в информационных системах ГБУЗ «Ленинская ЦРБ» с использованием средств автоматизации осуществляется в соответствии с требованиями ПП №1119 и ПП №211, нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

3.2. Оператором осуществляется определение уровня защищенности информационных систем в соответствии с ПП №1119 в зависимости от категории обрабатываемых данных, их количества.

3.3. Мероприятия по обеспечению безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с приказом ФСТЭК России от 18.02.2013 №21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», а также от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3.4. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации информационных систем, включающих акт по установлению уровня защищенности данных, инструкции пользователя, администратора, по организации антивирусной защиты, и других нормативных и методических документов;
- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с частной моделью угроз безопасности персональных данных;
- охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

3.5. ГБУЗ «Ленинская ЦРБ» прекращает обработку персональных данных или обеспечивает прекращение их обработки лицом, действующим по поручению ГБУЗ «Ленинская ЦРБ», в случае:

- изменения, признания утратившими силу нормативно-правовых актов, устанавливающих правовые основания обработки персональных данных;
- изменения или расторжения соглашений, заключенных ГБУЗ «Ленинская ЦРБ» во исполнение нормативно-правовых актов, на основании которых осуществляется обработка персональных данных;
- выявление неправомерной обработки персональных данных осуществляемой ГБУЗ «Ленинская ЦРБ» или лицом, действующим по поручению ГБУЗ «Ленинская ЦРБ»;
- достижение цели обработки персональных данных;
- отзыва субъектом персональных данных согласия на обработку его персональных данных, если в соответствии с законодательством Российской Федерации обработка персональных данных допускается только с согласия субъекта персональных данных.

4. ОТВЕТСТВЕННОСТЬ

Работники ГБУЗ «Ленинская ЦРБ», допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут

дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.