Приложение № 1
к Приказу СПб ГБУЗ «ГП №27»
№619/О от 29.12.2018г.

«СОГЛАСОВАНО»	**УТВЕРЖДАЮ»**
Председатель профкома	**Главный врач**
СПб ГБУЗ «ГП №27»	**СПб ГБУЗ «ГП №27»**
_____ Л.П. Тарусина	**_____ А.А. Команенко**
«___» _____ 2018г.	**«___» _____ 2018г.**

ПОЛИТИКА
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И РЕАЛИЗУЕМЫХ ТРЕБОВАНИЯХ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
СПб ГБУЗ «ГП №27»

Настоящая Политика обработки персональных данных и реализуемых требованиях к защите персональных данных СПб ГБУЗ «ГП №27» (далее — Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных и действует в отношении всей информации, которую учреждение (далее - оператор), может получить в рамках осуществления своей деятельности. Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных».

В Политике определены требования к персоналу оператора, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных (ИСПДн) оператора.

Целью настоящей Политики является обеспечение безопасности объектов защиты оператора, его работников, субъектов ПДн в информационных системах от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационной системы, а также выполнение законодательства Российской Федерации о персональных данных.

Политика распространяется на данные полученные как до, так и после подписания настоящей Политики.

Политика является публичным документом.

СПб ГБУЗ «ГП №27» обеспечивает защиту обрабатываемых ПДн от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями 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 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование,

распространение персональных данных, а также иных несанкционированных действий. Должно осуществляться своевременное обнаружение и реагирование на УБПДн, предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Информация и связанные с ней ресурсы должны быть доступны для субъектов ПДн.

Требования настоящей Политики распространяются на всех работников оператора (штатных, временных, работающих по контракту и т.п.), а также пациентов, их родителей (законных представителей) и всех прочих лиц (подрядчики, аудиторы и т.п.).

Для целей настоящей Политики используются следующие основные понятия:

- 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;

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

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

- субъект (субъект персональных данных**)** - физическое лицо (пациенты и их родители (законные представители)), потребитель услуг СПб ГБУЗ «ГП №27»;

- 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. В рамках настоящей Политики оператором признается СПб ГБУЗ «ГП №27»;

- конфиденциальность персональных данных - операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

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

- использование персональных данных - действия (операции) с персональными данными, совершаемые должностным лицом оператора в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

- блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных работников, в том числе их передачи;

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

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

- общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

- информация - сведения (сообщения, данные) независимо от формы их представления;

- документированная информация - зафиксированная на материальном носителе путем документирования информации с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

Основные права и обязанности оператора

Оператор вправе:

1. Отстаивать свои интересы в суде,
2. Предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.),
3. Отказать в предоставлении персональных данных в случаях, предусмотренных законом,
4. Использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством РФ.

Обязанности оператора.

1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»,
2. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в законе,
3. Сведения, касающиеся обработки персональных данных субъекта, должны быть предоставлены субъекту персональных данных по его запросу оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных,
4. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных законом, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных соответствующую информацию.

Основные права и обязанности субъекта.

Субъект персональных данных согласно законодательству Российской Федерации, имеет право:

- получать информацию, касающуюся обработки своих персональных данных;
- требовать уточнения своих 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;

- требовать перечень обрабатываемых персональных данных, имеющихся в Организации и источник их получения;

- получать информацию о сроках обработки персональных данных, в том числе о сроках их хранения;

- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- требовать прекращение обработки своих персональных данных в случаях, предусмотренных законодательством Российской Федерации;

- обжаловать действия или бездействие оператора в судебном порядке в случае нарушения им порядка обработки персональных данных субъекта,

- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Цели сбора персональных данных

Цель сбора персональных данных определена Уставом СПб ГБУЗ «ГП №27» и состоит в осуществлении комплекса действий, направленных на достижение цели, в т.ч. оказание медицинских услуг населению, а также реализация обязанностей, возложенных на работодателя.

Оператор осуществляет обработку персональных данных в следующих целях:

1. Работники: содействие в трудовой деятельности, обеспечение личной безопасности, учет результатов исполнения договорных обязательств, осуществление безналичных платежей на счет работника, обеспечение работоспособности и сохранности ресурсов и имущества работодателя, осуществление коллективного взаимодействия и совместного использования информационных ресурсов, аттестация, повышение квалификации, а также наиболее полное исполнение обязательств и компетенций в соответствии с Трудовым кодексом Российской Федерации и другими нормативно-правовыми актами Российской Федерации в сфере трудовых отношений,

2. пациенты, их родители (законные представители): с целью исполнения требований законодательства РФ (Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и других нормативно-правовых актов Российской Федерации), договорных отношений.

Правовое основание обработки персональных данных

Оператор осуществляет обработку персональных данных на основании:

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

2. Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ;

3. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

4. Устава СПб ГБУЗ «ГП №27»;

5. договоров, заключаемых между оператором и субъектом персональных данных;

6. согласия на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям оператора);

7. и иных нормативных актов.

Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

1. Субъекты персональных данных

В СПб ГБУЗ «ГП №27» обрабатываются персональные данные следующих категорий физических лиц (субъектов персональных данных):

- работников (лиц, состоящих в трудовых отношениях с оператором);
- работников по гражданско-правовым договорам;
- пациентов, их родителей (законных представителей);
- иных лиц, давших согласие на обработку своих персональных данных, либо сделавших общедоступными свои персональные данные или чьи персональные данные получены из общедоступного источника, а также в других случаях, предусмотренных законодательством Российской Федерации.

2. Объем и категории обрабатываемых персональных данных

Оператор обрабатывает следующие категории персональных данных:

2.1. Работники: фамилия, имя, отчество; данные паспорта (серия, номер, кем и когда выдан); дата и место рождения; адрес места жительства и регистрации; индивидуальный номер налогоплательщика (ИНН); страховое свидетельство государственного пенсионного страхования (СНИЛС); контактный телефон; сведения о доходах; информация об образовании; сведения о составе семьи; сведения о социальных льготах и др.

2.2. пациенты, их родители (законные представители): фамилия, имя, отчество, год рождения, месяц рождения, дата рождения, место рождения, адрес, состояние здоровья, частной (интимной) жизни, рост, вес, данные свидетельства о рождении, паспортные данные, данные медицинского полиса, СНИЛС, медицинской карты, место работы (учебы), социальное положение, номера телефонов, контактная информация и др.

Порядок и условия обработки персональных данных

1. Перечень действий с персональными данными.

Оператор осуществляет обработку (сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) персональных данных.

2. Способы обработки и сроки обработки

Обработка персональных данных проводится смешанным способом, с передачей по внутренней сети оператора, с передачей по информационно-телекоммуникационной сети «Интернет».

Трансграничная передача персональных данных не осуществляется.

Оператор может поручить обработку персональных данных третьим лицам в случаях, если:

- субъект дал согласие на осуществление таких действий (при наличии условий в договоре с третьим лицом о соблюдении им принципов и правил обработки персональных данных, предусмотренных Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных»;

- для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

- в других случаях, предусмотренных законодательством Российской Федерации.

3. Меры и методы, применяемые для защиты персональных данных.

Оператор принимает необходимые и достаточные правовые, организационные и технические меры для защиты персональных данных граждан - субъектов персональных данных.

К мерам, применяемым для защиты персональных данных, относятся:

- назначение лица, ответственного за организацию обработки персональных данных;
- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»;
- разработка документов, определяющих политику оператора в отношении обработки персональных данных, локальных документов по вопросам обработки персональных данных;
- ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, с требованиями к защите персональных данных, с документами, определяющими политику оператора в отношении обработки персональных данных, локальными документами по вопросам обработки персональных данных;
- опубликование в сети «Интернет» документа, определяющего политику оператора в отношении обработки персональных данных;
- систематическое осуществление оценки эффективности принимаемых мер по обеспечению безопасности персональных данных;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных;
- осуществление контроля над принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Методами защиты персональных данных являются:

- реализация разрешительной системы допуска к обработке персональных данных;
- ограничение доступа в помещения, где размещены технические средства, осуществляющие обработку персональных данных, а также хранятся носители информации;
- разграничение доступа к персональным данным;
- регистрация действий сотрудников, контроль несанкционированного доступа к персональным данным;
- использование защищенных каналов связи.

4. Требования к персоналу по обеспечению защиты персональных данных.

Работники оператора, являющиеся пользователями информационных систем персональных данных (ИСПДн), должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ПК.

Работник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Работники оператора, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей, логинов и паролей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Работники оператора должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Работники оператора должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами оператора, третьим лицам.

При работе с ПДн на ПК работники оператора обязаны обеспечить исключение возможности просмотра ПДн третьими лицами с мониторов.

При завершении работы на ПК сотрудники обязаны защитить монитор с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Работники оператора должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены под роспись с ответственностью, предусмотренной законодательством РФ.

Работники обязаны без промедления сообщать обо всех подозрительных случаях работы ПК, способные повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

Должностные обязанности работников, обрабатывающих персональные данные описаны в следующих документах:

- положении, регламентирующем порядок и условия обработки персональных данных работников оператора;
- должностной инструкции ответственного за организацию обработки персональных данных у оператора;
- должностной инструкции лица, непосредственно осуществляющего обработку ПДн (Ответственность лица, непосредственно осуществляющего обработку ПДн).

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 Уголовного Кодекса Российской Федерации).

Работники оператора несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях работниками оператора правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях сотрудников оператора.

5. Условия хранения и прекращения обработки персональных данных

ПДн Субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде.

ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах.

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

Срок или условие прекращения обработки персональных данных в СПб ГБУЗ «ГП №27»:

- ликвидация оператора или прекращение деятельности;
- истечение 75 лет – хранение персональных данных работников;
- по исполнению обязательств по договорам и в течение срока исковой давности;
- отзыв согласия, если иное не предусмотрено федеральным законодательством, либо в течение срока хранения документов согласно установленным срокам хранения для определенных категорий документов, если иное не предусмотрено федеральным законодательством.

Принципы обработки ПДн

Принципами обработки ПДн в инспекции являются:

– законная и справедливая основа обработки ПДн, законные способы обработки ПДн;

– недопущение объединения баз данных, содержащих ПДн, обработка которых осуществляется в несовместимых между собой целях;

– обработка только тех ПДн, которые отвечают целям обработки;

– соответствие содержания и объема обрабатываемых ПДн целям обработки, недопустимость избыточности обрабатываемых ПДн по отношению к заявленным целям обработки;

– обеспечение точности ПДн, их достаточности и актуальности по отношению к целям обработки ПДн;

– обеспечение принятия необходимых мер по удалению или уточнению неполных или неточных данных;

– осуществление хранения ПДн в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Конфиденциальность.

Инспекция и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Согласие субъекта ПДн на обработку своих персональных данных.

1. Субъект ПДн принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются учреждением.

2. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн учреждение вправе продолжить обработку персональных данных без согласия субъекта ПДн при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона «О персональных данных».

3. В случаях, предусмотренных федеральным законом, обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

В случае подтверждения факта неточности персональных данных или неправомерности их обработки персональные данные подлежат их актуализации оператором, а обработка должна быть прекращена, соответственно.

При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом "О персональных данных" или иными федеральными законами;
- иное не предусмотрено иным соглашением между оператором и субъектом персональных данных.

Оператор обязан сообщить субъекту персональных данных или его представителю информацию об осуществляемой им обработке персональных данных такого субъекта по запросу последнего.

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

ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается актом об уничтожении носителей, подписанным членами комиссии.

Ответственность за организацию обработки персональных данных

Ответственное лицо за организацию обработки персональных данных СПб ГБУЗ «ГП №27» назначается приказом главного врача учреждения.

Заключительное положение

1. Изменение Политики

Оператор имеет право вносить изменения в настоящую Политику. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее утверждения и размещения в общедоступном месте, если иное не предусмотрено новой редакцией Политики.

2. Обратная связь

СПб ГБУЗ «ГП №27», юридический адрес: Санкт-Петербург, Вознесенский пр., д.29, лит. А; эл. адрес: p27@zdrav.spb.ru; тел/факс 315-92-80