Приложение 1
к приказу ТФОМС Санкт-Петербурга
от 08 июня 2016 г. № 237-А

Политика государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга» в отношении обработки персональных данных

1. Общие положения.

1.1. Настоящая Политика государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга» в отношении обработки персональных данных (далее – Политика) определяет цели, задачи и основные мероприятия по обеспечению безопасности персональных данных в ТФОМС Санкт-Петербурга от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Политика является основой для разработки локальных нормативных актов ТФОМС Санкт-Петербурга по обеспечению безопасности персональных данных.

1.3. Настоящая Политика распространяется на работников ТФОМС Санкт-Петербурга, включая работников, трудящихся по договору подряда, а также на работников сторонних организаций, взаимодействующих с ТФОМС Санкт-Петербурга на основании соответствующих нормативных, правовых и организационно-распорядительных документов, физических лиц, находящихся в гражданско-правовых отношениях с ТФОМС Санкт-Петербурга.

2. Термины и принятые сокращения.

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.

Персональные данные (ПДн) - 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.

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.

КИС ТФОМС – корпоративная информационная система государственного учреждения «Территориальный фонд обязательного медицинского страхования Санкт-Петербурга», в которой производится автоматизированная обработка персональных данных.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Обработка персональных данных.

3.1. Обработка ПДн в ТФОМС Санкт-Петербурга осуществляется в соответствии со следующими законодательными актами Российской Федерации:

3.1.1. Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

3.1.2. Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации».

3.1.3. Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3.1.4. 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 ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

3.1.5. Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.1.6. Приказом Министерства здравоохранения и социального развития Российской Федерации от 25.01.2011 № 29н «Об утверждении порядка ведения персонифицированного учёта в сфере обязательного медицинского страхования».

3.1.7. Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

3.1.8. Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3.1.9. Постановлением Правительства Санкт-Петербурга от 30.01.2012 № 65 «Об утверждении положения о Территориальном фонде обязательного медицинского страхования Санкт-Петербурга».

3.1.10. Трудовым кодексом РФ и другими нормативными актами.

3.2. ТФОМС Санкт-Петербурга осуществляет обработку ПДн работников ТФОМС Санкт-Петербурга и лиц застрахованных по программе обязательного медицинского страхования (ОМС).

3.3. ПДн работников ТФОМС Санкт-Петербурга:

1) фамилия, имя, отчество (последнее – при наличии);
2) дата и место рождения;
3) пол;
4) семейное положение;
5) данные основного документа, удостоверяющего личность гражданина Российской Федерации на территории Российской Федерации;
6) данные регистрационного учета по месту жительства (пребывания);
7) ИНН;
8) СНИЛС страховой номер индивидуального лицевого счета в системе обязательного пенсионного страхования (при наличии);
9) номера банковских счетов, указанных работников для перечисления заработной платы;
10) размер заработной платы;

11) сведения о полученном образовании, ученых званиях и степенях, повышении квалификации;
12) занимаемая должность;
13) сведения и данные документов воинского учета.

3.4. ПДн лиц застрахованных по программе ОМС:

1) фамилия, имя, отчество;
2) пол;
3) дата рождения;
4) место рождения;
5) гражданство;
6) данные документа, удостоверяющего личность;
7) место жительства;
8) место регистрации;
9) страховой номер индивидуального лицевого счета (СНИЛС), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования;
10) номер полиса обязательного медицинского страхования застрахованного лица;
11) данные о страховой медицинской организации, выбранной застрахованным лицом;
12) дата регистрации в качестве застрахованного лица;
13) статус застрахованного лица (работающий, неработающий);
14) персонифицированный учет сведений о медицинской помощи, оказанной застрахованным лицам:
    - номер полиса обязательного медицинского страхования застрахованного лица;
    - медицинская организация, оказавшая соответствующие услуги;
    - виды оказанной медицинской помощи;
    - условия оказания медицинской помощи;
    - сроки оказания медицинской помощи;
    - объемы оказанной медицинской помощи;
    - стоимость оказанной медицинской помощи;
    - диагноз;
    - профиль оказания медицинской помощи;
    - медицинские услуги, оказанные застрахованному лицу, и примененные лекарственные препараты;
    - примененные медико-экономические стандарты;

- специальность медицинского работника, оказавшего медицинскую помощь;
- результат обращения за медицинской помощью;
- результаты проведенного контроля объемов, сроков, качества и условий предоставления медицинской помощи.

3.5. Цели обработки ПДн ТФОМС Санкт-Петербурга:

1) осуществление персонифицированного учета сведений о застрахованных лицах и оказанной им медицинской помощи;
2) ведение регионального сегмента единого регистра застрахованных лиц;
3) реализация приоритетных национальных проектов в сфере здравоохранения;
4) формирование системы учета и отчетности и иных информационных ресурсов в сфере обязательного медицинского страхования граждан в Российской Федерации;
5) контроль объемов, сроков, качества и условий предоставления медицинской помощи в рамках обязательного медицинского страхования;
6) осуществление контроля за использованием средств обязательного медицинского страхования медицинскими и страховыми медицинскими организациями;
7) регулирование трудовых отношений с работниками ТФОМС Санкт-Петербурга.

3.6. Способы обработки ПДн и перечень совершаемых с ними действий:

1) путём их сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи, предоставления, обезличивания, блокирования, удаления и (или) уничтожения;
2) с использованием средств автоматизации и без них (смешанная обработка ПДн).

3.7. Обработка ПДн осуществляется путем смешанной обработки ПДн в КИС ТФОМС. Полученные в ходе обработки информации данные передаются:

1) по закрытой (без выхода в сеть Интернет) внутренней сети, с доступом работникам ТФОМС Санкт-Петербурга определенным Приказом ТФОМС Санкт-Петербурга;
2) по защищенным каналам сети общего пользования Интернет в территориальные фонды ОМС, Федеральный фонд ОМС, медицинские учреждения, страховые медицинские организации Санкт-Петербурга, ФНС России по Санкт-Петербургу, Отделение пенсионного фонда России по Санкт-Петербургу, Фонд социального страхования.

3.8. КИС ТФОМС является информационной системой обрабатывающей специальные категории ПДн, так как в ней обрабатываются ПДн касающиеся состояния здоровья субъектов ПДн.

3.9. Хранение ПДн.

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

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

3.9.3. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах.

3.10. Уничтожение ПДн.

3.10.1. Уничтожение документов (носителей), содержащих ПДн производится путем сожжения, дробления (измельчения). Для уничтожения бумажных документов допускается применение шредера.

3.10.2. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

3.10.3. Уничтожение производится комиссией, утвержденной приказом ТФОМС. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

3.11. Сроки или условия прекращения обработки ПДн.

Основанием для прекращения обработки ПДн является прекращение деятельности ТФОМС Санкт-Петербурга, изменение действующего законодательства Российской Федерации, другие предусмотренные законодательством РФ основания.

4. Защита персональных данных.

4.1. В соответствии с требованиями нормативных документов в ТФОМС Санкт-Петербурга создана система защиты персональных данных (далее - СЗПДн), состоящая из подсистем правовой, организационной и технической защиты.

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

4.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПДн, разрешительной системы, защиты информации при работе с работниками и сторонними организациями.

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

4.5. Основными мерами защиты ПДн, используемыми в ТФОМС Санкт-Петербурга, являются:

4.5.1. Назначение лица ответственного за обработку ПД, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением в ТФОМС Санкт-Петербурга его работниками требований к защите ПДн.

4.5.2. Определение актуальных угроз безопасности ПДн при их обработке в КИС ТФОМС, и разработка мер и мероприятий по защите ПДн.

4.5.3. Разработка локальных нормативных актов в отношении обработки ПДн.

4.5.4. Установление правил доступа к ПДн, обрабатываемым в КИС ТФОМС, а также обеспечения регистрации и учета всех действий, совершаемых с ПДн в КИС ТФОМС.

4.5.5. Установление индивидуальных паролей доступа работников в информационную систему в соответствии с их должностными обязанностями.

4.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

4.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

4.5.8. Сертифицированные программные средства защиты информации от несанкционированного доступа.

4.5.9. Сертифицированные межсетевой экран и средство обнаружения вторжения.

4.5.10. Соблюдаются условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

4.5.11. Обнаружение фактов несанкционированного доступа к персональным данным и принятия мер.

4.5.12. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

4.5.13. Обучение работников ТФОМС Санкт-Петербурга, непосредственно осуществляющих обработку ПДн, в рамках требований законодательства Российской Федерации в части защиты персональных данных, в том числе документам, определяющими политику ТФОМС Санкт-Петербурга в отношении обработки персональных данных, локальным нормативным актам по вопросам обработки персональных данных.

4.5.14. Осуществление внутреннего контроля и аудита.

5. Правила рассмотрения запросов субъектов ПДн или их представителей.

5.1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн.

Сведения предоставляются субъекту ПДн или его представителю оператором при обращении либо при получении запроса субъекта ПДн или его представителя.

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

5.2. Сведения должны быть предоставлены субъекту ПДн оператором в доступной форме. В них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

5.3. Повторное обращение субъекта ПДн к оператору в целях получения сведений и ознакомления с ПДн возможно не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса.

6. Согласие на обработку ПДн субъектов ПДн.

6.1. Согласие на обработку ПДн субъектов ПДн относящихся к гражданам РФ застрахованных в ОМС и гражданам РФ, получивших медицинскую помощь в соответствии со статьями 9, 43, 44 Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании» и пунктом 2 части 1 статьи 6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» не требуется.

6.2. Согласие на обработку ПДн работников ТФОМС Санкт-Петербурга.

В случае трудовых отношений, обработка ПДн осуществляется только с согласия субъекта ПДн оформляемом в письменной форме.

Согласие на обработку ПДн может быть отозвано субъектом ПДн.

7. Осуществление внутреннего контроля соответствия обработки ПДн.

Внутренний контроль соответствия обработки ПДн проводится ежегодно комиссией по защите информации, утвержденной приказом директора ТФОМС Санкт-Петербурга.

Основными вопросами внутреннего контроля соответствия обработки ПДн являются:

1) соответствие документации по вопросам обработки ПДн реальному положению дел;
2) соблюдение лицами, допущенными к обработке ПДн, всех требований, установленных локальными нормативными актами в ТФОМС Санкт-Петербурга.
3) проверка соблюдения защиты прав субъектов ПДн, путем анализа их обращений и действий, совершаемых работниками ТФОМС Санкт-Петербурга, в связи с этими обращениями.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю докладывает ответственный за организацию обработки ПДн в ТФОМС Санкт-Петербурга.