Приложение №1
к Распоряжению
№144.1 от 03.07.2017

Политика обработки и защиты персональных данных в «Медицинском центре «XXI век»

1. Термины и определения

Информационная безопасность — свойство информации сохранять конфиденциальность, целостность и доступность (в некоторых случаях, также свойство сохранять аутентичность, подотчетность, неотказуемость и надежность).

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

Материальный носитель — бумажные носители (оригиналы документов, содержащие персональные данные; документы в печатной форме, полученные на основе информации, хранимой в информационных системах – выписки, отчеты, и т.п.), а также электронные носители информации, в том числе, отчуждаемые (USB flash, CD диски, и т.п.).

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

Субъект ПДн — физическое лицо, персональные данные которого обрабатываются в Медицинском центре «XXI век».

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

2. Общие положения

Политика обработки и защиты персональных данных в Медицинском центре «XXI век» (далее — «Политика») определяет принципы, цели и условия обработки персональных данных (далее — ПДн), а также стратегию их защиты в Медицинском центре «XXI век» (далее — Медицинский центр «XXI век»).

Настоящая Политика является основным руководящим внутренним документом Медицинского центра «XXI век», определяющим требования, предъявляемые в отношении обработки и обеспечения безопасности ПДн.

Внутренние документы Медицинского центра «XXI век», регламентирующие вопросы, рассматриваемые в настоящей Политике, должны разрабатываться с учетом положений настоящей Политики и не противоречить им.

Политика разработана в целях реализации положений законодательства Российской Федерации в отношении обработки ПДн, а также требований нормативных и методических документов по защите ПДн.

3. Принципы обработки персональных данных в Медицинском центре «XXI век»

Обработка ПДн в Медицинском центре «XXI век» осуществляется на основе принципов:

- законности и справедливости целей и способов обработки ПДн;
- соответствия целей обработки ПДн законным целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Медицинского центра «XXI век»;
- соответствия объема и содержания обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- точности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих ПДн;
- хранения ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, или устанавливающий срок хранения федеральный закон, договор, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;
- уничтожения ПДн по достижении целей их обработки, в случае утраты необходимости в достижении целей обработки или по окончании срока хранения ПДн, установленного федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

Обработка ПДн в Медицинском центре «XXI век» осуществляется путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн.

4. Цели и правовые основания обработки персональных данных

Медицинский центр «XXI век» осуществляет обработку ПДн в целях:

- принятия решения о трудоустройстве;
- обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- принятия решения о заключении договора на оказание услуг, заключение и исполнение такого договора).

Правовыми основаниями для обработки ПДн являются, в том числе:

- Федеральный закон Российской Федерации от 30 ноября 1994 г. № 51-ФЗ «Гражданский кодекс Российской Федерации (часть первая)»;
- Федеральный закон Российской Федерации от 26 января 1996 г. № 14-ФЗ «Гражданский кодекс Российской Федерации (часть вторая)»;
- Федеральный закон Российской Федерации от 31 июля 1998 года № 146-ФЗ «Налоговый кодекс Российской Федерации»;

– Федеральный закон Российской Федерации от 30 декабря 2001 г. № 197-ФЗ «Трудовой кодекс Российской Федерации»;

– Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

– Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – «ФЗ «О персональных данных»);

– Федеральный закон от 1 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

– Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановление правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Устав Медицинского центра «XXI век».

Медицинский центр «XXI век» обрабатывает ПДн, ставшие известными ему в связи с реализацией задач и целей деятельности, а также в результате, но не ограничиваясь:

– заключения трудовых или гражданско-правовых договоров (договоров об оказании услуг, договор подряда и др.);

– поступления в Медицинский центр «XXI век» письменных, в том числе электронных, обращений, запросов, заявлений, жалоб, ходатайств;

– заключения соглашений о сотрудничестве;

– заключения соглашений о конфиденциальности;

– получения учредительных документов юридических лиц, доверенностей, уполномочивающих физических лиц представлять интересы юридического или физического лица в его отношениях с Медицинским центром «XXI век», иных документов для последующего заключения с Медицинским центром «XXI век» гражданско-правовых договоров и договоров оказания услуг;

– получения любых иных документов от Контрагентов, необходимых для заключения Медицинским центром «XXI век» договоров с такими лицами;

– осуществления иных действий, предусмотренных действующим законодательством Российской Федерации или внутренними политиками Медицинского центра «XXI век».

5. Обрабатываемые персональные данные

Медицинский центр «XXI век» обрабатывает ПДн следующих субъектов ПДн:

– соискатели вакантной должности;

– сотрудник/бывший сотрудник;

– клиент (пациент);

– законный представитель пациента;

– третье лицо, которому пациент/законный представитель пациента предоставил право запроса и получения сведений;

– представитель контрагента.

В соответствии с положениями Постановления Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в Медицинском центре «XXI век» обрабатываются следующие ПДн:

– специальные категории персональных данных - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

– общедоступные персональные данные — персональные данные, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Закона о персональных данных;

– иные категории персональных данных — персональные данные, не отнесенные к категориям: специальные, биометрические и общедоступные персональные данные.

Медицинский центр «XXI век» может разместить в сервисах счетчики, которые используются для анализа cookie файлов, для сбора и обработки статистических данных об использовании сервисов, обеспечения работоспособности сервисов в целом или их отдельных функций в частности.

Медицинский центр «XXI век» определяет структуру файла cookie, параметры работы счетчиков и может изменять их без предварительного уведомления Пользователя.

Полный перечень ПДн, обрабатываемых в Медицинском центре «XXI век», определяется отдельным документом «Перечень персональных данных», утверждаемым директором Медицинского центра «XXI век».

6. Условия обработки персональных данных

Обработка ПДн Медицинского центра «XXI век» допускается в следующих случаях:

– обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;

– обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации;

– обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн;

– обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн;

– осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Медицинский центр «XXI век» вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этой стороной договора (поручения на обработку ПДн). Лицо, осуществляющее обработку ПДн по поручению Медицинского центра «XXI век», обязано соблюдать принципы и правила обработки ПДн, предусмотренные ФЗ «О персональных данных».

В поручении третьему лицу Медицинским центром «XXI век» указываются цели обработки и перечень действий (операций) с ПДн, которые могут быть совершены данным лицом, устанавливается его обязанности по обеспечению конфиденциальности и безопасности ПДн при их обработке, а также требования к защите обрабатываемых ПДн в соответствии с ФЗ «О персональных данных».

Медицинский центр «XXI век» не осуществляет трансграничную передачу ПДн.

Обработка ПДн прекращается Медицинским центром «XXI век» в следующих случаях:

– при выявлении неправомерных действий с ПДн в срок, не превышающий трех рабочих дней с даты такого выявления, Медицинский центр «XXI век» устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений Медицинский центр «XXI век» в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, уничтожает ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Медицинский центр «XXI век» уведомляет субъекта ПДн или его законного представителя, а в случае, если обращение или запрос были направлены в уполномоченный орган по защите прав субъектов ПДн, также этот орган;

– при достижении цели обработки ПДн Медицинский центр «XXI век» незамедлительно прекращает обработку ПДн и уничтожает соответствующие ПДн в срок, не превышающий тридцати рабочих дней с даты достижения цели обработки ПДн;

– при отзыве субъектом ПДн согласия на обработку своих ПДн Медицинский центр «XXI век» прекращает обработку ПДн и уничтожает (за исключением ПДн, которые хранятся в соответствии с действующим законодательством) ПДн в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва. Об уничтожении ПДн Медицинский центр «XXI век» уведомляет субъекта ПДн.

7. Согласие на обработку персональных данных

Получение и обработка ПДн в случаях, предусмотренных ФЗ «О персональных данных», осуществляется в Медицинском центре «XXI век» с согласия субъекта ПДн, в том числе в письменной форме.

Письменное согласие субъекта ПДн должно включать:

– фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– наименование и адрес Медицинского центра «XXI век»;

– цель обработки ПДн;

– перечень ПДн, на обработку которых дается согласие субъекта ПДн;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Медицинского центра «XXI век», если обработка будет поручена такому лицу;

– перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых в Медицинском центре «XXI век» способов обработки ПДн;

– срок, в течение которого действует согласие, а также способ его отзыва;

– подпись субъекта ПДн.

Типовые формы согласий на обработку ПДн утверждаются приказом директора Медицинского центра «XXI век».

Субъект ПДн дает Медицинскому центру «XXI век» согласие на обработку своих ПДн свободно, в своей воле и своем интересе. Согласие на обработку ПДн может быть отозвано субъектом ПДн путем направления в Медицинский центр «XXI век» письменного заявления в свободной форме. В этом случае Медицинский центр «XXI век» обязуется прекратить обработку, а также уничтожить все имеющиеся в Медицинский центр «XXI век» ПДн в сроки, установленные ФЗ «О персональных данных».

Медицинский центр «XXI век» вправе обрабатывать ПДн без согласия субъекта ПДн (или при отзыве субъектом ПДн указанного согласия) при наличии оснований, указанных в пп. 2-11 ч. 1 ст. 6, ч. 2. ст. 10 и ч. 2 ст. 11 ФЗ «О персональных данных».

Передача ПДн третьим лицам осуществляется Медицинский центр «XXI век» с согласия субъекта ПДн в соответствии с требованиями действующего законодательства.

8. Права субъектов персональных данных

Субъект ПДн имеет право на получение информации, касающейся обработки в Медицинском центре «XXI век» его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Медицинским центром «XXI век»;
- правовые основания и цели обработки ПДн;
- цели и применяемые в Медицинском центре «XXI век» способы обработки ПДн;
- наименование и местонахождение Медицинского центра «XXI век», сведения о лицах (за исключением сотрудников Медицинского центра «XXI век»), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Медицинским центром «XXI век» или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных ФЗ «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Медицинского центра «XXI век», если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами.

Медицинский центр «XXI век» предоставляет указанную информацию на основании соответствующего письменного заявления субъекта ПДн (далее — Заявление), поданного по адресу места нахождения Медицинского центра «XXI век»: г. Санкт-Петербург, проспект Большой Сампсониевский, дом 45, или направленного на почтовый адрес Медицинского центра «XXI век»: 194044, г. Санкт-Петербург, проспект Большой Сампсониевский, дом 45. Заявление должно содержать номер основного документа, удостоверяющего личность субъекта ПДн, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Медицинским центром «XXI век» (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн в Медицинском центре «XXI век», подпись субъекта ПДн. Медицинский центр «XXI

век» обязуется сообщить субъекту ПДн информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн в течение тридцати дней с даты получения Заявления субъекта ПДн.

Субъект ПДн вправе требовать от Медицинского центра «XXI век» 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.

Если субъект ПДн считает, что Медицинский центр «XXI век» осуществляет обработку его ПДн с нарушением требований ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие Медицинского центра «XXI век» в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами Российской Федерации.

9. Обеспечение безопасности персональных данных

Медицинский центр «XXI век» не несет ответственности, если ПДн стали известны неограниченному кругу лиц по вине самого субъекта ПДн.

Для обеспечения безопасности ПДн в Медицинском центре «XXI век» принимаются организационные и технические меры, включающие в том числе:

- назначение лица, ответственного за организацию обработки ПДн, определение его функций и полномочий;
- назначение лица, ответственного за обеспечение безопасности ПДн, определение его функций и полномочий;
- разработка и поддержание актуальности комплекта внутренних нормативных документов в отношении обработки и защиты ПДн;
- проведение оценки вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ «О персональных данных», а также соотношение указанного вреда с принимаемыми мерами по безопасности ПДн;
- ознакомление сотрудников Медицинского центра «XXI век», непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации и внутренних нормативных документов Медицинского центра «XXI век» в отношении обработки и защиты ПДн, периодическое обучение вопросам обработки и защиты ПДн;
- определение угроз безопасности ПДн при их обработке в ИСПДн;
- учет сотрудников, допущенных к обработке ПДн;
- учет материальных носителей ПДн;
- применение технических средств защиты информации;
- периодический внутренний контроль, а также внешний аудит соответствия обработки ПДн требованиям ФЗ «О персональных данных» и принятым в соответствии с ним нормативно-правовым актам;
- обнаружение фактов несанкционированного доступа к ПДн и принятием мер;

– восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

– контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

Комплекс мероприятий и технических средств по обеспечению безопасности ПДн в Медицинском центре «XXI век» формулируется с учетом результатов оценки возможного вреда субъекту ПДн, который может быть нанесен в случае нарушения безопасности его ПДн, актуальности угроз безопасности ПДн, а также установления уровня защищенности ПДн.

10. Контроль за соблюдением законодательства РФ и локальных нормативных актов Медицинского центра «XXI век» в области персональных данных

Контроль за соблюдением подразделениями Медицинского центра «XXI век» локальных нормативных актов Медицинского центра «XXI век» в области ПДн осуществляется с целью проверки соответствия процессов обработки и защиты ПДн требованиям законодательства РФ в области ПДн, а также выявления возможных каналов утечки и несанкционированного доступа к ПДн.

Внутренний контроль за соблюдением подразделениями Медицинского центра «XXI век» требований законодательства РФ и локальных нормативных актов Медицинского центра «XXI век» в области ПДн осуществляется лицами, ответственными за обработку и защиту ПДн в Медицинском центре «XXI век».

Сотрудники Медицинского центра «XXI век», виновные в нарушении норм, регулирующих обработку и защиту ПДн, установленных в Медицинском центре «XXI век», могут быть привлечены к дисциплинарной, материальной, гражданско-правовой, административной или уголовной ответственности в соответствии с законодательством РФ.

11. Заключительные положения

Настоящая Политика является публичным, равнодоступным документом и предоставляется для ознакомления неограниченному кругу лиц на сайте Медицинского центра «XXI век»: https://www.mc21.ru/.

Внесение изменений в настоящую Политику может вызвано изменениями в законодательстве Российской Федерации, внутренних документах Медицинского центра «XXI век», информационных системах ПДн, системе защиты ПДн.

Все изменения и дополнения, внесенные в настоящую Политику, утверждаются в порядке, предусмотренном в Медицинском центре «XXI век».

Все сотрудники Медицинского центра «XXI век» подлежат обязательному ознакомлению с настоящей Политикой и несут предусмотренную законодательством Российской Федерации ответственность за нарушение её положений.

Вопросы толкования настоящей Политики необходимо адресовать в Медицинский центр «XXI век».