УТВЕРЖДАЮ

Директор ООО «БиоЛинк»

\_\_\_\_\_\_\_\_\_\_\_\_ Корниенко А.А.

Приказ № \_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2015г.

ПОЛОЖЕНИЕ

Об обработке персональных данных в ООО «БиоЛинк»

Настоящее Положение об обработке персональных данных (далее – Положение) Общества с ограниченной ответственностью «БиоЛинк» (ООО «БиоЛинк») регламентирует порядок обработки персональных данных, предоставляемых пациентами (их законными представителями), пользователями/посетителями сайта [www.biolinklab.ru](http://www.biolinklab.ru), иными категориями физических лиц, предоставляющими свои персональные данные. Настоящее Положение является открытым документом и предназначено для ознакомления неограниченного круга лиц.

Положение разработано в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных (далее - ПДн) в ООО «БиоЛинк».

Положение разработано в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями), Федерального закона Российской Федерации от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (с изменениями и дополениями) и Постановлением Правительства Российской Федерации от 01.11.2012г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иных нормативно-правовых актов.

В Положении определены перечень субъектов ПДн, ПДн которых обрабатываются в ООО «БиоЛинк», цели сбора и обработки ПДн, условия обработки ПДн и их передача третьим лицам, методы защиты ПДн, реализуемые в ООО «БиоЛинк», права субъектов ПДн и ответственность ООО «БиоЛинк», как оператора. Список, используемых сокращений:

ИС - информационная система

ПДн - персональные данные

ИСПДн - ИС персональных данных

СЗИ - средства защиты информации

1. ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящего Положения является обеспечение обработки ПДн в соответствии с требованиями действующего законодательства в сфере защиты ПДн, обеспечение безопасности ПДн, обрабатываемых ООО «БиоЛинк», от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн. Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий. При обработке ПДн ООО «БиоЛинк» придерживается следующих принципов:

* соблюдение законности получения, обработки, хранения, а также других действий с ПДн;
* обработка ПДн исключительно в целях, перечисленных в п.3 настоящего Положения;
* хранение ПДн, обработка которых осуществляется с несвязанными между собой целями, в различных базах данных;
* сбор только тех ПДн, которые минимально необходимы для достижения заявленных целей обработки;
* выполнение мер по обеспечению безопасности ПДн, их точности, достаточности и других характеристик при обработке и хранении;
* соблюдение прав субъекта ПДн на доступ к его ПДн;
* соблюдение требований по уничтожению либо обезличиванию ПДн по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

ООО «БиоЛинк» не производит обработку ПДн субъектов ПДн в целях продвижения товаров, работ, услуг на рынке, а также в целях политической, религиозной агитации.

В ООО «БиоЛинк» принятие решений на основании исключительно автоматизированной обработки ПДн не производится.

2. ОБРАБАТЫВАЕМЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

ИСПДн, принадлежащие ООО «БиоЛинк», предназначены для обработки ПДн:

физических лиц (их законных представителей), получающих медицинские услуги в ООО «БиоЛинк» в соответствии с договором оказания платных медицинских услуг, иными видами договоров;

персональные данные физических лиц (их законных представителей), обрабатываемые в связи с функционированием сайта www.mcststus.ru.

Под обработкой ПДн в ООО «БиоЛинк» понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

В ООО «БиоЛинк» допускается обработка сведений о состоянии здоровья только в случае необходимости такой обработки в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг и при условии доступа к таким данным исключительно медицинского персонала.

Обработка сведений о состоянии здоровья в иных целях или немедицинским персоналом возможна только при наличии согласия субъекта персональных данных.

Обработка иных специальных категорий персональных данных допускается только при наличии согласия субъекта персональных данных. К специальным категориям персональных данных относятся: расовая принадлежность; политические взгляды; философские убеждения; состояние интимной жизни; национальная принадлежность; религиозные убеждения.

3. ЦЕЛИ СБОРА И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Цели обработки персональных данных в ООО «БиоЛинк» определены в соответствии с действующим законодательством и Уставом ООО «БиоЛинк». Основными целями обработки персональных данных являются:

− исполнение обязанностей, как работодателя, в соответствии с законодательством Российской Федерации: содействие в трудоустройстве, обучении и продвижении по службе, ведение кадрового делопроизводства, обеспечение личной безопасности работника, контроль количества и качества выполняемой работы, обеспечение сохранности имущества, обеспечение медицинского и социального страхования, охраны труда, организация командирования работников;

− исполнение гражданско-правовых договоров на оказание медицинских и иных услуг, стороной которого, либо выгодоприобретателем по которому, является субъект персональных данных;

− архивное хранение документов в соответствии с законодательством Российской Федерации, в том числе выдача архивных справок по требованию субъекта персональных данных или его законного представителя.

4. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИХ ПЕРЕДАЧА ТРЕТЬИМ ЛИЦАМ

4.1. Обработка персональных данных

Обработка ПДн в ООО «БиоЛинк» происходит как неавтоматизированным, так и автоматизированным способом. Любая обработка персональных данных должна проводиться таким образом, чтобы было возможным определить перечень лиц, имеющих право на доступ и обработку персональных данных.

К обработке ПДн в ООО «БиоЛинк» допускаются только сотрудники, прошедшие определенную процедуру допуска, к которой относятся:

− ознакомление сотрудника под роспись с локальными нормативными актами ООО «БиоЛинк» (положения, инструкции и т.д.), строго регламентирующими порядок и процедуру работы с ПДн;

− взятие с сотрудника подписки о соблюдении конфиденциальности в отношении ПДн при работе с ними;

− получение сотрудником и использование в работе индивидуальных атрибутов доступа к информационным системам (далее - ИС) ООО «БиоЛинк», содержащим в себе ПДн. При этом каждому сотруднику выдаются минимально необходимые для исполнения трудовых обязанностей права на доступ в информационные системы ПДн (далее - ИСПДн).

Сотрудники, имеющие доступ к ПДн, получают только те ПДн, которые необходимы и достаточны им для выполнения конкретных трудовых обязанностей.

4.2. Хранение персональных данных

ПДн хранятся в бумажном и электронном виде. В электронном виде ПДн хранятся в базах данных и на технических средствах ИСПДн ООО «БиоЛинк», а также в архивных копиях баз данных этих ИСПДн.

При хранении ПДн соблюдаются организационные и технические меры, обеспечивающие их сохранность и исключающие несанкционированный доступ к ним. К ним относятся:

− назначение сотрудника, ответственного за обработку ПДн;

− для информационных систем персональных данных, обрабатывающих специальные категории персональных данных, назначается должностное лицо, ответственное за обеспечение безопасности персональных данных в информационных системах (администратор безопасности);

− ограничение физического доступа к местам обработки персональных данных, хранения носителей персональных данных;

− учет всех информационных систем и электронных и бумажных носителей, а также архивных копий;

Места хранения носителей персональных данных, порядок хранения, учета и уничтожения к ним регламентируются внутренними документами ООО «БиоЛинк», утверждаемыми директором.

4.3. Передача персональных данных

Для целей обработки данных ООО «БиоЛинк» может передавать ПДн исключительно своим сотрудникам и третьим лицам, подписавшим обязательство по обеспечению конфиденциальности и безопасности полученных сведений, а также непосредственно субъектам персональных данных или их законным представителям.

Передача персональных данных субъектам персональных данных или их законным представителям производится только после письменного обращения в ООО «БиоЛинк» и при предоставлении документа удостоверяющего личность субъекта или законного представителя. Факт выдачи персональных данных субъектам фиксируется ответственным за организацию обработки ПДн.

Так же с письменного согласия пациента или его законного представителя допускается разглашение сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях.

Предоставление сведений, составляющих врачебную тайну, без согласия пациента или его законного представителя допускается только по основаниям, предусмотренным действующим законодательством Российской Федерации:

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 Федерального закона Российской Федерации от 21 ноября 2011 г. №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 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;

4) в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 Федерального закона Российской Федерации от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 Федерального закона Российской Федерации от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», для информирования одного из его родителей или иного законного представителя;

5) в целях расследования несчастного случая на производстве и профессионального заболевания;

6) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований регуляторов по защите персональных данных;

7) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с Федеральным законом Российской Федерации от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

Передача персональных данных третьим лицам в остальных случаях возможна только с согласия субъекта ПДн и только с целью исполнения обязанностей перед субъектом ПДн в рамках договора, либо когда такая обязанность у ООО «БиоЛинк» наступает в результате требований федерального законодательства или при поступлении запроса от уполномоченных государственных органов. В последнем случае ООО «БиоЛинк» ограничивает передачу ПДн запрошенным объемом. Передача данных, в данном случае, должна фиксироваться в соответствующем журнале ответственным лицом.

Передача персональных данных третьим лицам возможна только в рамках соглашения об информационном обмене или поручения оператора на обработку ПДн.

Исключением являются случаи предоставления информации в соответствии с требованиями о предоставлении информации, предъявленными уполномоченными государственными органами в соответствии с действующим законодательством.

В случае заключения поручения на обработку персональных данных с третьими лицами, в таком поручение 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 со статьей 19 Федерального закона №152-ФЗ «О персональных данных».

При передаче персональных данных в электронном виде третьим лицам по открытым каналам связи ООО «БиоЛинк» обязано принимать все необходимые меры по защите передаваемой информации в соответствии с требованиями нормативно-методической документации регуляторов.

5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Обеспечение безопасности персональных данных в ООО «БиоЛинк» достигается следующими мерами:

− назначением сотрудника, ответственного за организацию обработки ПДн;

− разработкой частной модели угроз безопасности ПДн и модели нарушителя;

− определением на основе разработанной частной модели угроз безопасности требуемого уровня защищенности;

− назначение должностного лица, ответственного за обеспечение безопасности персональных данных;

− определением списка лиц, допущенных к работе с ПДн;

− определением правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;

− разработкой и утверждением локальных нормативных актов ООО «БиоЛинк», регламентирующих порядок обработки ПДн, разработкой для пользователей и ответственных лиц рабочих инструкций;

− проведением периодического обучения и повышением осведомленности сотрудников в области защиты ПДн;

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

− физической защитой технических средств ИСПДн;

− контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

Меры по защите персональных данных, обрабатываемых без средств автоматизации, определяется в соответствии с Постановлением правительства Российской Федерации №687от 15.09.2008 г. «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6. ПРАВА

Субъект персональных данных имеет право на получение информации, касающейся обработки его ПДн, за исключением случаев, когда право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами.

В частности, субъект ПДн имеет право на получение следующей информации, касающейся обработки его ПДн:

− подтверждение факта обработки ПДн;

− правовые основания и цели обработки ПДн;

− цели и применяемые способы обработки ПДн;

− сведения о лицах (за исключением сотрудников ООО «БиоЛинк»), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора или на основании федерального закона;

− обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения;

− сроки обработки ПДн, в том числе сроки их хранения;

− порядок осуществления субъектом ПДн своих прав;

− иные сведения, предусмотренные Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами.

Получить данную информацию субъект ПДн может, обратившись с письменным запросом в ООО «БиоЛинк». Ответ, содержащий запрашиваемую информацию, либо мотивированный отказ в ее предоставлении направляется по адресу, указанному в запросе, в течение 30 дней.

Порядок обработки запросов субъектов ПДн по выполнению их законных прав в ООО «БиоЛинк» производится согласно утвержденному внутреннему документу, разработанному в соответствии с действующим законодательством в области защиты ПДн и подконтролен сотруднику, ответственному за обработку ПДн.

7. ОБЯЗАННОСТИ

ООО «БиоЛинк» обязуется осуществлять обработку ПДн только с согласия субъектов ПДн, за исключением случаев, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

При сборе ПДн ООО «БиоЛинк» обязуется по запросу субъекта ПДн предоставлять информацию, касающуюся обработки его ПДн, перечисленную в п.6 настоящего Положения. В случае если предоставление ПДн является обязательным в соответствии с федеральным законом, ООО «БиоЛинк» обязуется разъяснять субъекту ПДн юридические последствия отказа предоставить его ПДн.

Если ПДн получены не от субъекта ПДн, ООО «БиоЛинк» до начала обработки таких ПДн обязуется предоставить субъекту ПДн сведения, касающиеся обработки его ПДн в соответствии с требованиями Федерального закона от 27 июля 2006г. г. № 152-ФЗ «О персональных данных». В случаях, если ООО «БиоЛинк» не является оператором ПДн, полученных от субъектов ПДн, обязанность по предоставлению субъекту ПДн соответствующих сведений возлагается на оператора ПДн, от которого эти данные получены.

ООО «БиоЛинк» при обработке ПДн обязуется принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении ПДн.

Описание принимаемых мер приведено в п.5 настоящего Положения. ООО «БиоЛинк» обязуется отвечать на запросы субъектов ПДн, их представителей, а также уполномоченного органа по защите прав субъектов ПДн касательно обрабатываемых ПДн в соответствии с требованиями законодательства.

В случае предоставления субъектом ПДн, либо его представителем сведений, подтверждающих факты каких-либо нарушений в процессе обработки ПДн, ООО «БиоЛинк» обязуется устранить данные нарушения в течение семи рабочих дней и уведомить субъекта ПДн о внесенных изменениях и предпринятых мерах.

В случае достижения целей обработки ПДн ООО «БиоЛинк» обязуется прекратить обработку ПДн и уничтожить ПДн в течение 30 дней, если иное не предусмотрено условиями договора, заключенного с субъектом ПДн, либо иным соглашением.

ООО «БиоЛинк» обязуется уведомлять уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных». В случае изменения предоставленных сведений ООО «БиоЛинк» обязуется предоставлять актуализированные сведения в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки ПДн.

8. ОТВЕТСТВЕННОСТЬ

ООО «БиоЛинк» несет ответственность за разработку, введение и действенность соответствующих требованиям законодательства норм, регламентирующих получение, обработку и защиту ПДн.

9. ИЗМЕНЕНИЕ ПОЛИТИКИ

В целях обеспечения пригодности, адекватности и эффективности, настоящая Политика подлежит пересмотру не реже одного раза в год с момента ее опубликования.

Политика подлежит внеплановому пересмотру в случае существенных изменений

деятельности ООО «МЦ «XXI век» - Новосибирск», изменений в законодательстве в

области защиты ПДн и иных подобных случаях.