УТВЕРЖДАЮ

Главный врач
ГБУЗ ЯО «ОЦМП»

_____ С.В. Гамаянова

«17» июня 2016 г.

ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных работников государственного бюджетного учреждения здравоохранения Ярославской области «Областной центр медицинской профилактики»

1 Термины и определения

1.1 Ниже приведён перечень определений, используемых при подготовке настоящего Положения.

Безопасность информации — состояние защищённости информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, то есть сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

Доступ к информации — возможность получения информации и ее использования.

Доступность информации — состояние информации, характеризуемое способностью автоматизированной системы обеспечить беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защита информации от несанкционированного доступа или воздействия — деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию).

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

Информация — сведения (сообщения, данные) независимо от их формы представления.

Информация ограниченного доступа — информация, доступ к которой ограничен федеральными законами.

Конфиденциальная информация — информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к такой информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Несанкционированный доступ — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средством вычислительной техники или автоматизированной системой.

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.

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

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Средства вычислительной техники — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Технические средства информационной системы персональных данных — средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки 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.

Целостность информации — состояние защищённости информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки и хранения.

2 Основные положения

2.1 Настоящее Положение принято в целях определения основных принципов обработки и защиты персональных данных (далее по тексту – ПДн) работников государственного бюджетного учреждения здравоохранения Ярославской области «Областной центр медицинской профилактики» (далее по тексту – ГБУЗ ЯО «ОЦМП») от несанкционированного доступа, неправомерного использования или утраты.

2.2 Настоящее Положение разработано на основе и во исполнение Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», положений Трудового кодекса Российской Федерации.

2.3 Настоящее Положение является обязательным для исполнения всеми сотрудниками ГБУЗ ЯО «ОЦМП», имеющими доступ к ПДн работников.

2.4 Все работники ГБУЗ «ОЦМП» должны быть ознакомлены под роспись с настоящим Положением и иными документами ГБУЗ ЯО «ОЦМП», устанавливающими порядок обработки ПДн работников.

2.5 Настоящее Положение вступает в силу с даты его утверждения и действует до его отмены либо замены новым Положением.

3 Понятие и состав ПДн работника

3.1 ПДн работника – любая информация, к прямо или косвенно относящаяся определенному или определяемому работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, гражданство, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, указания о возможности занимать лицом те или иные должности, сведения о предыдущих местах работы и другая информация, необходимая работодателю в связи с организацией трудовых отношений между работником и работодателем.

3.2 ПДн работника составляют:

– сведения о работнике, позволяющие идентифицировать его и получить о нем дополнительную информацию;

– служебные и иные сведения, связанные с профессиональной деятельностью работника.

4 Документы, содержащие ПДн

4.1 Информация, представляемая работником при поступлении (приеме) на работу в ГБУЗ ЯО «ОЦМП», должна иметь документальную форму.

4.2 При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

– паспорт или иной документ, удостоверяющий личность;

– трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;

– страховое свидетельство государственного пенсионного страхования (при его наличии);

– документы воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

– документ об образовании, о квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);

– свидетельство о присвоении идентификационного номера налогоплательщика (при его наличии у работника);

– справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (при поступлении на работу, связанную с деятельностью, к осуществлению которой не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию).

В отдельных случаях с учетом специфики работы может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

4.3 После оформления трудового договора и приема на работу специалист по кадрам ГБУЗ ЯО «ОЦМП» заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

– табельный номер работника, идентификационный номер налогоплательщика, номер страхового свидетельства государственного пенсионного страхования, сведения о характере и виде работы, пол работника;

– общие сведения (фамилия, имя, отчество работника, дата рождения, место рождения, гражданство, сведения о знании иностранных языков, сведения об образовании, профессия, сведения о стаже работы, сведения о составе семьи, сведения о паспорте, адрес прописки и фактического проживания, телефон, номер трудового договора);

– сведения о воинском учете;

– данные о приеме на работу.

В дальнейшем в личную карточку вносятся:

– сведения о занимаемых работником должностях;

– сведения о переводах на другую работу;

– сведения об аттестации работника;

– сведения о повышении квалификации;

– сведения о профессиональной переподготовке;

– сведения о наградах (поощрениях), почетных званиях;

– сведения об отпусках;

– сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством.

4.4 ПДн работников содержатся также и в иных документах, сопровождающих процесс оформления трудовых отношений (трудовой деятельности) работников ГБУЗ ЯО «ОЦМП»:

– подлинники и копии приказов (распоряжений) по личному составу;

– командировочные удостоверения;

– документы, содержащие сведения о расчете оплаты труда, доплатах, надбавках, единовременных выплатах;

– документы, предоставляемые самим работником (заявления, справки, больничные листы);

– графики отпусков.

4.5 ПДн работников ГБУЗ ЯО «ОЦМП» могут содержаться в документах бухгалтерского учета и отчетности (первичных учетных документах, актах, журналах, книгах, ведомостях, платежных поручениях, отчетных формах и т. д.).

4.6 ПДн работников ГБУЗ ЯО «ОЦМП» могут быть включены в документацию, связанную с организацией работы структурных подразделений ГБУЗ ЯО «ОЦМП» (штатное расписание (штатная расстановка); приказы, распоряжения, указания руководства ГБУЗ ЯО «ОЦМП», иные внутренние нормативные акты; внутренние списки различного назначения).

5 Принципы обработки ПДн работника в ГБУЗ ЯО «ОЦМП»

5.1 В ГБУЗ ЯО «ОЦМП» обработка ПДн работника осуществляется исключительно в целях обеспечения условий трудового договора, заключенного между работодателем и работником, обеспечения соблюдения законов Российской Федерации и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

5.2 В ГБУЗ ЯО «ОЦМП» не допускается принятие решений, затрагивающих интересы работника, основанных исключительно на ПДн работника, полученных в электронном виде либо в результате их автоматизированной обработки.

6 Создание ПДн работника

6.1 Документы, содержащие ПДн работника, создаются путём:

– копирования оригиналов документов (паспорт, документ об образовании) либо получения заверенных копий;

– получения (создания) оригиналов документов (трудовая книжка, личная карточка);

– внесения сведений в документы, файлы, учетные формы;

– дополнения документов путем формирования (расчета) сведений на основе имеющихся данных с использованием средств автоматизации.

6.2 Необходимые ПДн работника на основании приказов (распоряжений) главного врача ГБУЗ ЯО «ОЦМП» по личному составу вносятся специалистом по кадрам ГБУЗ ЯО «ОЦМП» в специализированные электронные системы.

6.3 Дальнейшая обработка ПДн работника (в процессе трудовой деятельности) осуществляется как на бумажных носителях, в неавтоматизированном режиме, так и с использованием средств автоматизации.

6.4 Доступ к сведениям, содержащим ПДн работника, разрешён лицам, непосредственно использующим ПДн работника в служебных целях. Перечень долж-

ностных лиц, которые могут иметь доступ к ПДн работников, определён в пункте 7.1 настоящего положения.

7 Перечень лиц, имеющих доступ к ПДн работников

7.1 Доступ к ПДн работников могут иметь следующие сотрудники ГБУЗ ЯО «ОЦМП»:

- Специалист по кадрам ГБУЗ ЯО «ОЦМП»;
- главный бухгалтер ГБУЗ ЯО «ОЦМП»;
- главный врач ГБУЗ ЯО «ОЦМП»;
- сотрудники отдела ИТ ГБУЗ ЯО «ОЦМП».

7.2 Перечень лиц, имеющих доступ к ПДн работников, утверждается приказом главного врача ГБУЗ ЯО «ОЦМП».

7.3 Уполномоченные лица имеют право доступа к тем и только тем ПДн работников, которые необходимы для выполнения конкретных функций в соответствии с должностными инструкциями указанных лиц.

8 Хранение ПДн работников

8.1 Личные дела (личные карточки) работников хранятся у специалиста по кадрам ГБУЗ ЯО «ОЦМП». Трудовая книжка, документы воинского учёта хранятся в запертом металлическом сейфе.

8.2 Хранение бумажных и электронных носителей информации, содержащих ПДн работников, должно осуществляться в закрытых помещениях, шкафах и сейфах. При приеме посетителей данные носители информации должны быть убраны в стол, шкаф, сейф либо иное место с целью исключения возможности несанкционированного доступа к ним. Места хранения носителей, содержащих ПДн, утверждаются приказом главного врача ГБУЗ ЯО «ОЦМП».

8.3 В электронном виде ПДн работников могут содержаться в файлах (в том числе файлах баз данных):

- на АРМ специалиста по кадрам ГБУЗ ЯО «ОЦМП»;
- на АРМ главного бухгалтера ГБУЗ ЯО «ОЦМП»;
- на АРМ сотрудника отдела ИТ ГБУЗ ЯО «ОЦМП».

8.4 В случае увольнения сотрудника его ПДн должны быть выведены из рабочей базы данных в архив. Личное дело (личная карточка) уволенного сотрудника также передается в архив.

9 Возможность получения ПДн у третьих лиц

9.1 ПДн работника, обрабатываемые в ГБУЗ ЯО «ОЦМП», предоставляет сам работник.

9.2 Получение ПДн работника от третьей стороны допускается только при условии предварительного уведомления работника и наличия его письменного согласия. Работник должен быть уведомлен о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа работника дать письменное согласие на их получение.

10 Возможность предоставления ПДн третьим лицам

10.1 Передача сотрудниками ГБУЗ ЯО «ОЦМП» ПДн работника третьей стороне возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

10.2 Предоставление сотрудниками ГБУЗ ЯО «ОЦМП» ПДн работников третьим лицам без соответствующего их согласия возможно в следующих случаях:

– в целях предупреждения угрозы жизни и здоровья работника;

– при поступлении официальных запросов в соответствии с положениями Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»;

– при поступлении официальных запросов из налоговых органов, органов Пенсионного Фонда России, органов Фонда социального страхования, судебных органов.

10.3 ПДн работника не должны сообщаться по телефону кому бы то ни было.

10.4 При передаче ПДн работника работодатель обязан предупредить лиц, получающих ПДн работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Лица, получающие ПДн работника, обязаны соблюдать режим конфиденциальности и обеспечивать безопасность полученных ПДн.

11 Защита ПДн

11.1 Защита ПДн представляет собой регламентированный технологический процесс, предупреждающий нарушение доступности, целостности (достоверности, полноты) и конфиденциальности ПДн и, в конечном счете, обеспечивающий безопасность информации в процессе управленческой и производственной деятельности организации.

11.2 Защита ПДн работника от неправомерного их использования, разглашения или утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральными законами. В отношении информационных систем ПДн и отдельных технических средств, на которых обрабатываются ПДн работников ГБУЗ ЯО «ОЦМП», должен быть проведен полный комплекс технических мероприятий по защите ПДн от несанкционированного доступа в соответствии с требованиями действующих на территории Российской Федерации руководящих и нормативно-методических документов по защите конфиденциальной информации (ПДн).

11.3 Комплекс организационных мер по защите ПДн работников ГБУЗ ЯО «ОЦМП» включает:

– ограничение круга лиц, доступ к ПДн работников которым необходим для выполнения служебных обязанностей (перечень таких сотрудников утверждается главным врачом ГБУЗ ЯО «ОЦМП», доступ в строгом соответствии с указанным перечнем обеспечивается с помощью организационных и (или) технических мер);

– ограничение круга лиц, имеющих доступ в помещения, в которых расположены технические средства, участвующие в обработке ПДн, и хранятся электронные либо бумажные носители ПДн, исключение неконтролируемого пребывания в таких помещениях лиц, не имеющих допуска к ПДн работников ГБУЗ ЯО «ОЦМП»;

– сопровождение посетителей и иных посторонних лиц на территории организации (в пределах контролируемой зоны) постоянными сотрудниками организации либо оборудование мест пребывания посетителей системой видеонаблюдения;

– оснащение помещений, занимаемых ГБУЗ ЯО «ОЦМП», системой охранной сигнализации либо обеспечение охраны помещений в нерабочее время;

– уведомление лиц, допущенных к ПДн работников, об обработке ими информации ограниченного доступа и об ответственности за нарушение установленных требований к порядку обработки и защите такой информации (под роспись);

– проведение инструктажей по безопасности с сотрудниками, имеющими доступ к ПДн работников, проверок знания сотрудниками требований нормативно-методических документов по защите информации;

– контроль за соблюдением установленного в организации порядка обработки ПДн и обращения с носителями ПДн, проведение разбирательств по фактам несоблюдения установленных в организации требований по защите ПДн работников;

– размещение рабочих мест (средств отображения информации, средств графической обработки информации) способом, исключающим несанкционированный просмотр выводимой информации лицами, не имеющими допуска к ПДн;

– обеспечение своевременного вывода ПДн из обработки (перевода на архивное хранение либо уничтожения).

11.4 Защита ПДн работников, содержащихся на электронных носителях

Файлы, содержащие ПДн работников ГБУЗ ЯО «ОЦМП» (в том числе файлы баз данных), должны храниться в специально выделенных каталогах на определенных средствах вычислительной техники. На данные файлы/каталоги должны быть установлены права доступа в соответствии с разрешительной системой доступа (матрицей доступа) к защищаемым ресурсам (матрица доступа к защищаемым ресурсам должна быть документально зафиксирована и составлена таким образом, чтобы сотрудники имели доступ к тем и только тем ПДн, которые необходимы им для выполнения своих служебных обязанностей).

Хранение файлов, содержащих ПДн, на внешних (отчуждаемых) носителях разрешается только в случае ведения учета данных носителей. Копирование файлов, содержащих ПДн, на неучтенные внешние носители информации запрещено и является нарушением трудовой дисциплины.

12 Права и обязанности работника как субъекта ПДн

12.1 В целях обеспечения защиты своих ПДн работники имеют право на:

– полную информацию об их ПДн и обработке этих данных;

– свободный бесплатный доступ к своим ПДн, включая право на получение копий любой записи, содержащей ПДн работника, за исключением случаев, предусмотренных федеральным законодательством. Право работника на доступ к своим ПДн ограничивается в случае, если предоставление ПДн нарушает конституционные права и свободы других лиц;

– исключение или исправление неверных или неполных ПДн, а также данных, обрабатываемых с нарушением федерального законодательства. При отказе работодателя исключить или исправить ПДн работник имеет право заявить в письмен-

ной форме работодателю о своём несогласии, обосновав соответствующим образом такое несогласие. ПДн оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения. Работник имеет право требовать от работодателя уведомления всех лиц, которым ранее были сообщены неверные или неполные ПДн работника, обо всех произведённых в них изменениях или исключениях из них. Неправомерные действия или бездействие работодателя при обработке и защите ПДн работника могут быть обжалованы в суд;

– получение подтверждения факта обработки ПДн оператором, а также сведений о цели и правовых основаниях такой обработки, способах обработки ПДн, применяемых оператором, сроках обработки ПДн (в том числе сроках их хранения), возможности трансграничной передачи ПДн; перечня обрабатываемых ПДн и сведений об источнике их получения; сведений о лице, обрабатывающем по поручению оператора ПДн работника;

– получение сведений о лицах, которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора, заключенного с оператором, или федерального закона (за исключением работников оператора).

12.2 В свою очередь, работник обязан:

– передавать работодателю или его представителю комплекс достоверных, документированных ПДн, состав которых установлен трудовым законодательством и иными федеральными законами;

– своевременно сообщать работодателю об изменении своих ПДн.

13 Обязанности работодателя

13.1 В случае необходимости работодатель обязан разъяснить работнику порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов. Работодатель обязан рассмотреть возражение работника в течение тридцати дней со дня его получения и уведомить его о результатах рассмотрения такого возражения.

13.2 Если обязанность предоставления ПДн работником установлена федеральным законом, работодатель обязан разъяснить работнику юридические последствия отказа предоставить свои ПДн.

13.3 Если ПДн были получены не от работника за исключением случаев, если ПДн были предоставлены оператору в связи с исполнением договора, на основании федерального закона или если ПДн сделаны общедоступными субъектом ПДн (либо получены из общедоступного источника), работодатель до начала обработки таких ПДн обязан предоставить работнику следующую информацию[1]:

– наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

– цель обработки ПДн и ее правовое основание;

– предполагаемые пользователи ПДн;

[1] Если субъект ПДн не уведомлен об обработке его ПДн соответствующим оператором.

- права работника в области защиты ПДн;
- источник получения ПДн.

13.4 Работодатель обязан безвозмездно предоставить работнику возможность ознакомления с ПДн, относящимися к соответствующему работнику, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие ПДн по предоставлении работником сведений, подтверждающих, что ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах работодатель обязан уведомить работника и третьих лиц, которым ПДн этого работника были переданы.

13.5 В случае выявления неточных ПДн или неправомерной обработки ПДн работодатель обязан осуществить блокирование ПДн, относящихся к соответствующему работнику, с момента получения такой информации на период проверки.

13.6 В случае подтверждения факта неточности ПДн или неправомерной обработки ПДн работодатель на основании соответствующих документов обязан в течение семи рабочих дней обеспечить уточнение ПДн, снять их блокирование и принять меры по уведомлению об изменении ПДн тех лиц, которым ПДн работника были переданы.

13.7 В случае выявления неправомерных действий с ПДн работодатель в срок, не превышающий трех рабочих дней с даты такого выявления, обязан прекратить неправомерную обработку ПДн. В случае, если обеспечить правомерность обработки ПДн невозможно, работодатель в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить ПДн. Об устранении допущенных нарушений или об уничтожении ПДн работодатель обязан уведомить работника.

13.8 В случае достижения цели обработки ПДн работодатель обязан прекратить обработку ПДн и уничтожить соответствующие ПДн в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено федеральными законами (в частности, законодательством об архивном деле), договором или соглашением, стороной которого является работник.

14 Ответственность за нарушение установленных требований по защите ПДн работников ГБУЗ ЯО «ОЦМП»

14.1 Руководитель, разрешающий доступ сотрудника к документам, файлам, базам данных или их частям, содержащим ПДн, несет персональную ответственность за данное разрешение.

14.2 Сотрудник, получающий доступ к документам, файлам, базам данных или их частям, содержащим ПДн, несет персональную ответственность за любые действия, совершаемые с информацией или ее носителями.

14.3 Лица, виновные в нарушении установленных норм, регулирующих порядок обработки и мероприятия по защите ПДн работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

14.4 За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом Российской Федерации дисциплинарные взыскания.

14.5 Нарушение неприкосновенности частной жизни (в том числе незаконный сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения, наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с Уголовным Кодексом Российской Федерации.

15 Ознакомлены

С правилами ознакомлен, правила изучены и понятны.

№ п/п	Ф.И.О. сотрудника	Должность	Дата ознакомления	Личная подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				