Приложение 1

к приказу №86

от «18» 02 2015 г.

УТВЕРЖДАЮ

Главный врач КГБУЗ «ККЦО»

«19» 02 2015 г. _____/Коваленко В.Л.

Политика информационной безопасности в области обработки и защиты персональных данных КГБУЗ «Краевого клинического центра онкологии»

Хабаровск 2015

Оглавление

1. Общие положения

Настоящая Политика в области обработки и защиты персональных данных Краевого государственного бюджетного учреждения здравоохранения «Краевого клинического центра онкологии» (далее – Центр):

– Разработана в целях обеспечения реализации требований законодательства РФ в области обработки персональных данных (далее – ПДн) субъектов персональных данных;

– Раскрывает основные категории персональных данных, обрабатываемых Центром, цели, способы и принципы обработки Центром персональных данных, права и обязанности Центра при обработке персональных данных, права субъектов персональных данных, а также перечень мер, применяемых учреждением в целях обеспечения безопасности персональных данных при их обработке;

– Является общедоступным документом, декларирующим концептуальные основы деятельности учреждения при обработке персональных данных.

Целью настоящей Политики является обеспечение безопасности объектов защиты учреждения от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных (далее - УБПДн).

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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Политика определяет:

– Категории персональных данных, обрабатываемых в информационных системах персональных данных (далее - ИСПДн) учреждения, и источники их получения;

– Правовые основания обработки персональных данных;

– Цели обработки персональных данных;

– Принципы обработки персональных данных;

– Способы обработки персональных данных и перечень совершаемых с ними действий;

– Условия обработки персональных данных;

– Условия прекращения обработки персональных данных;

– Меры, принимаемые учреждением для обеспечения конфиденциальности и безопасности персональных данных при их обработке в ИСПДн учреждения.

Настоящая Политика вступает в силу с момента его утверждения руководством Центра и действует бессрочно, до замены ее новой Политикой.

Политика подлежит пересмотру в случае изменения законодательства Российской Федерации о персональных данных. Изменения в Политику вносятся на основании отдельных приказов главного врача Центра.

Состав объектов защиты представлен в «Перечне персональных данных, подлежащих защите».

Состав ИСПДн подлежащих защите, представлен в «Отчете о результатах проведения внутренней проверки».

Требования настоящей Политики распространяются на всех сотрудников Центра (штатных, временных, работающих по контракту и т.п.), сотрудников клинических кафедр, а также всех прочих лиц (подрядчики, аудиторы и т.п.)

2. Принципы и условия обработки персональных данных

2.1 Категории персональных данных, обрабатываемых в ИСПДн Центра и источники их получения

В ИСПДн Центра обрабатываются:

– персональные данные граждан;

– специальные категории персональных данных, содержащих сведения о состоянии здоровья граждан и об оказанной им медицинской помощи;

– персональные данные медицинских работников, включенных в региональный сегмент Федерального регистра медицинских работников - врачей терапевтов участковых и медицинских сестер участковых врачей - терапевтов участковых, осуществляющих дополнительную медицинскую помощь в учреждении, оказывающих первичную медико-санитарную помощь;

– персональные данные работников, заключивших с Центром трудовые договоры;

– персональные данные физических лиц, заключивших с Центром договоры подряда, оказания услуг;

– персональные данные физических лиц, содержащиеся в медицинских свидетельствах о смерти.

Источниками персональных данных, обрабатываемых в ИСПДн учреждения, являются:

– документы, удостоверяющие личность;

– данные страхового полиса ОМС (ДМС);

– страховой номер Индивидуального лицевого счета в Пенсионном фонде России (СНИЛС);

– идентификационный номер налогоплательщика (ИНН);

– военный билет;

– диплом об образовании (сведения об образовании и профессиональной подготовке);

– данные о состоянии здоровья.

Центр не несет ответственности за достоверность и актуальность персональных данных, полученных от других организаций (общественных объединений) в соответствии с законодательством Российской Федерации.

2.2 Правовые основания обработки персональных данных

Обработка персональных данных в ИСПДн Центра осуществляется на основании:

– Конституции Российской Федерации;

– Трудового кодекса Российской Федерации;

– Гражданского кодекса Российской Федерации;

– Налогового кодекса Российской Федерации;

– Гражданского процессуального кодекса Российской Федерации;

– Уголовно-процессуального кодекса Российской Федерации

– Федеральный закон от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;

– Федеральный закон от 29.11.2010 N 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

– постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных»;

– Положение об обработке персональных данных, осуществляемых без использования средств автоматизации, утверждённое постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687;

– Федерального закона от 24.07.1998 г. № 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»;

– Федерального закона от 24.07.2009 г. № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального

страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования»;

– Федерального закона от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

– Федерального закона от 19.05.1995 № 81-ФЗ «О государственных пособиях гражданам, имеющим детей»;

– Федерального закона от 15.12.2001 № 166-ФЗ «О государственном пенсионном обеспечении в Российской Федерации»;

– Федерального закона от 17.12.2001 № 173-ФЗ «О трудовых пенсиях в Российской Федерации»;

– Приказа Министерства здравоохранения и социального развития Российской Федерации (далее - Минздравсоцразвития России) от 17.01.2008г. № 14н «О порядке ведения федерального регистра медицинских работников - врачей-терапевтов участковых, врачей-педиатров участковых, врачей общей практики (семейных врачей) и медицинских сестер участковых врачей-терапевтов участковых, медицинских сестер участковых врачей-педиатров участковых, медицинских сестер врачей общей практики (семейных врачей)»;

– Приказа Минздравсоцразвития от 26.04.2012г. №406н «Об утверждении порядка выбора гражданином медицинской организации при оказании ему медицинской помощи в рамках программы государственных гарантий бесплатного оказания гражданам медицинской помощи»;

– Приказа Министерства по налогам и сборам Российской Федерации № БГ-3-09/171, ФОМС № 8 от 02.03.2004г. «Об утверждении порядка информационного взаимодействия территориальных регистрирующих (налоговых) органов и территориальных фондов обязательного медицинского страхования при государственной регистрации юридических лиц и индивидуальных предпринимателей в электронном виде»;

– Приказа Министерства здравоохранения и социального развития РФ от 26.12.2008 № 782н «Об утверждении и порядке ведения медицинской документации, удостоверяющих случаи рождения и смерти».

2.3 Цели обработки персональных данных

Обработка персональных данных Центром осуществляется на основании отраслевых нормативно-правовых актов с соблюдением требований законодательства в области защиты персональных данных.

Цель обработки персональных данных:

- ведение учета в кадровом делопроизводстве;
- обеспечение правильного и своевременного расчета и начисления заработной платы и других выплат работнику;
- обеспечение соответствия требованиям Трудового, Гражданского, Налогового кодексов Российской Федерации, а также федеральным законам и другим нормативным правовым актам Российской Федерации;
- обработка ПДн осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну (п.2 ст.10 ФЗ-152);
- выполнения функций, полномочий и обязанностей, возложенных на Центр законодательством об основах охраны здоровья граждан РФ, законодательством об обязательном медицинском страховании, налоговым законодательством, законодательством по воинскому учету, социальному обеспечению, социальному страхованию, законодательством о судопроизводстве, об исполнительном производстве;

– в целях обеспечения реализации предусмотренных законодательством Российской Федерации полномочий органа государственной власти Хабаровского края в сфере здравоохранения.

2.4 Принципы обработки персональных данных

Обработка персональных данных в ИСПДн Центра осуществляется в соответствии со следующими принципами:

– законность обработки персональных данных;

– прекращение обработки персональных данных после достижения конкретных, заранее определенных и законных целей;

– недопустимость обработки персональных данных, несовместимой с целями их сбора;

– недопустимость объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

– осуществление обработки только тех персональных данных, которые отвечают целям их обработки;

– соответствие содержания и объема обрабатываемых персональных данных заявленным целям их обработки;

– обеспечение точности, достаточности, а в необходимых случаях и актуальности персональных данных по отношению к целям их обработки;

– хранение персональных данных 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;

– уничтожение либо обезличивание обрабатываемых персональных данных по достижению целей их обработки или в случае утраты

необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.5 Способы обработки персональных данных и перечень совершаемых с ними действий

Обработка персональных данных в ИСПДн Центра осуществляется:

– путем их сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи, предоставления, обезличивания, блокирования, удаления и (или) уничтожения;

– с использованием средств автоматизации и без них (смешанная обработка персональных данных).

2.6 Условия обработки персональных данных

Обработка персональных данных в ИСПДн Центра осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных».

Центр производит обработку персональных данных при наличии хотя бы одного из следующих условий:

– обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

– обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

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

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

– обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

– осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - общедоступные персональные данные);

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

– персональные данные сделаны общедоступными субъектом персональных данных;

– обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

– обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что

обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

– обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия, уполномоченными на это органами, в соответствии с законодательством РФ;

– обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные ФЗ-152.

При осуществлении трансграничной передачи персональных данных субъекта персональных данных, Центр обязан убедиться в том, что иностранным государством, на территорию которого предполагается осуществлять передачу персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления такой передачи.

Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

– наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

– исполнения договора, стороной которого является субъект персональных данных.

Передача, предоставление персональных данных, обрабатываемых в ИСПДн Центра, другим организациям осуществляется в соответствии с законодательством Российской Федерации.

2.7 Условия прекращения обработки и сроки хранения персональных данных

Центр прекращает обработку персональных данных или обеспечивает прекращение их обработки лицом, действующим по поручению Центра, в случае:

– Изменения, признания утратившими силу нормативных правовых, нормативных актов, устанавливающих правовые основания обработки персональных данных;

– Изменения или расторжения соглашений, заключенных учреждением во исполнение нормативных правовых актов, на основании которых осуществляется обработка персональных данных;

– Выявления неправомерной обработки персональных данных, осуществляемой учреждением или лицом, действующим по поручению учреждения (в срок, не превышающий трех рабочих дней с даты этого выявления). В случае, если обеспечить правомерность обработки персональных данных невозможно, Центр в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение;

– Достижения цели обработки персональных данных (в срок, не превышающий тридцати дней с даты достижения цели, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных);

– Отзыва субъектом персональных данных согласия на обработку его персональных данных, если в соответствии с Федеральным законом от 27.07.2006г. №152-ФЗ «О персональных данных» обработка персональных данных допускается только с согласия субъекта персональных данных (в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных).

По истечении сроков, определенных законодательством Российской Федерации, личные дела работников и иные документы передаются на архивное хранение на срок 75 лет. При этом, на организацию архивного хранения, комплектования, учет и использование архивных документов, содержащих персональные данные работников, действие Федерального закона «О персональных данных» не распространяется, и соответственно, обработка указанных сведений не требует соблюдения условий, связанных с получением согласия на обработку персональных данных.

2.8 Меры по обеспечению конфиденциальности и безопасности персональных данных при их обработке в ИСПДн Центра

Центр в целях обеспечения конфиденциальности и безопасности персональных данных при их обработке в ИСПДн принимает необходимые правовые, организационные и технические меры, предусмотренные Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Центр 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.

2.9 Сбор, обработка и защита персональных данных

2.9.1. Порядок получения (сбора) персональных данных

Все персональные данные субъекта следует получать у него лично с его письменного согласия, кроме случаев, определенных в настоящем разделе Политики и иных случаях, предусмотренных законами.

Согласие субъекта на использование его персональных данных хранится в бумажном виде в его медицинской карте.

Согласие субъекта на обработку персональных данных действует в течение всего срока действия договора, а также в течение 5 лет с даты прекращения действия договорных отношений субъекта с Центром. По истечении указанного срока действие согласия считается продленным на каждые следующие пять лет при отсутствии сведений о его отзыве.

Если персональные данные субъекта возможно получить только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Третье лицо, предоставляющее персональные данные субъекта, должно обладать согласием субъекта на передачу персональных данных Центром. Центр обязан получить подтверждение от третьего лица, передающего персональные данные субъекта персональных данных о том, что персональные данные передаются с согласия субъекта. Центр обязан при взаимодействии с третьими лицами заключить с ними соглашение о конфиденциальности информации, касающейся персональных данных субъектов.

Центр обязан сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

Обработка персональных данных субъектов без их согласия осуществляется в следующих случаях:

- Персональные данные являются общедоступными.

- По требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.
- Обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора.
- Обработка персональных данных осуществляется в целях заключения и исполнения договора, одной из сторон которого является субъект персональных данных.
- Обработка персональных данных осуществляется для статистических целей при условии обязательного обезличивания персональных данных.
- В иных случаях, предусмотренных законом.

2.9.2. Порядок обработки персональных данных

Субъект персональных данных предоставляет сотруднику Центра, ответственному за ведение регистрацию субъекта достоверные сведения о себе.

На основании полученной информации сотрудник Центра проверяет наличие данного субъекта, зарегистрированного в информационной системе. Если субъект отсутствует в информационной системе, то сотрудник заносит полную информацию о субъекте, после получения письменного согласия последнего. В случае наличия информации о субъекте в информационной системе – сверяет данные с ранее предоставленными (при необходимости вносит соответствующие изменения).

При определении объема и содержания, обрабатываемых персональных данных Центр должен руководствоваться требованиями Роскомнадзора, ФСБ, ФСТЭК и иных контролирующих органов, Конституцией Российской Федерации, закона о персональных данных, Трудовым кодексом Российской Федерации и иными федеральными законами.

2.9.3. Защита персональных данных

Под защитой персональных данных субъекта понимается комплекс мер (организационно-распорядительных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.

Защита персональных данных субъекта осуществляется за счёт Центра в порядке, установленном федеральным законом.

Центр при защите персональных данных субъектов принимает все необходимые организационно-распорядительные, юридические и технические меры, в том числе:

- Антивирусная защита.
- Анализ защищённости.
- Обнаружение и предотвращение вторжений.
- Управления доступом.
- Регистрация и учет.
- Обеспечение целостности.
- Шифровальные (криптографические) средства.
- Организация нормативно-методических локальных актов, регулирующих защиту персональных данных.

2.10 Блокировка, обезличивание, уничтожение персональных данных

2.10.1 Порядок блокировки и разблокировки персональных данных

Блокировка персональных данных субъектов осуществляется с письменного заявления субъекта персональных данных.

Блокировка персональных данных подразумевает:

- Запрет редактирования персональных данных.
- Запрет распространения персональных данных любыми средствами (e-mail, сотовая связь, материальные носители).

- Запрет использования персональных данных в массовых рассылках (sms, e-mail, почта).
- Изъятие бумажных документов, относящихся к субъекту персональных данных и содержащих его персональные данные из внутреннего документооборота Организации и запрет их использования.

Блокировка персональных данных субъекта может быть временно снята, если это требуется для соблюдения законодательства.

Разблокировка персональных данных субъекта осуществляется с его письменного согласия или заявления.

Повторное согласие субъекта персональных данных на обработку его данных влечет разблокирование его персональных данных.

2.10.2 Порядок обезличивания и уничтожения персональных данных

Обезличивание персональных данных субъекта происходит по письменному заявлению субъекта персональных данных, при условии, что все договорные отношения завершены и от даты окончания последнего договора прошло не менее 5 лет.

При обезличивании персональные данные в информационных системах заменяются набором символов, по которому невозможно определить принадлежность персональных данных к конкретному субъекту.

Бумажные носители документов при обезличивании персональных данных уничтожаются в установленном порядке с оформлением соответствующих актов.

Центр обязан обеспечить конфиденциальность в отношении персональных данных при необходимости проведения испытаний информационных систем на территории разработчика и произвести обезличивание персональных данных в передаваемых разработчику информационных системах.

Уничтожение персональных данных субъекта подразумевает прекращение какого-либо доступа к персональным данным субъекта.

При уничтожении персональных данных субъекта работники Организации не могут получить доступ к персональным данным субъекта в информационных системах.

Бумажные носители документов при уничтожении персональных данных уничтожаются, персональные данные в информационных системах обезличиваются. Персональные данные восстановлению не подлежат.

Операция уничтожения персональных данных необратима.

Срок, после которого возможна операция уничтожения персональных данных субъекта определяется окончанием срока указанным в настоящем пункте Политики.

2.11 Передача и хранение персональных данных

2.11.1 Передача персональных данных

Под передачей персональных данных субъекта понимается распространение информации по каналам связи и на материальных носителях.

При передаче персональных данных работники Организации должны соблюдать следующие требования:

- Не сообщать персональные данные субъекта в коммерческих целях. Обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи не допускается.
- Осуществлять передачу персональных данных субъектов в пределах Организации в соответствии с настоящим Положением, нормативно-технологической документацией и должностными инструкциями.
- Разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения должностных обязанностей.

– Передавать персональные данные субъекта представителям субъекта в порядке, установленном законодательством и нормативно-технологической документацией и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

2.11.2 Хранение и использование персональных данных

Под хранением персональных данных понимается существование записей в информационных системах и на материальных носителях.

Персональные данные субъектов обрабатываются и хранятся в информационных системах, а также на бумажных носителях в Организации.

Хранение персональных данных субъекта может осуществляться не дольше, чем этого требуют цели обработки, если иное не предусмотрено федеральными законами.

2.11.3 Сроки хранения персональных данных

Сроки хранения персональных данных субъектов, относящихся к трудовым правоотношениям, составляют 75 лет. (основание – Перечень типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения, утв. Росархивом 06.10.2000 г.).

Сроки хранения личных дел (заявления, автобиографии, копии приказов и выписки из них, копии личных документов, характеристики, листки по учету кадров, анкеты, аттестационные листы и др.) руководства Организации, членов контрольных органов, а также работников, имеющих государственные и иные звания, премии, награды, ученые степени и звания) - постоянно.

Документы (анкеты, автобиографии, листки по учету кадров, заявления, рекомендательные письма, резюме и др.) лиц, не принятых на работу хранятся 1 год.

Сроки хранения персональных данных субъектов, относящихся к доходам субъектов, составляют 4 года (основание – Статья 23 НК РФ).

Сроки хранения гражданско-правовых договоров, содержащих персональные данные субъектов, а также сопутствующих документов - 5 лет с момента окончания действия договоров (основание – Перечень типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения, утв. Росархивом 06.10.2000 г.).

В течение срока хранения персональные данные не могут быть обезличены или уничтожены.

По истечении срока хранения персональные данные могут быть обезличены в информационных системах и уничтожены на бумажном носителе.

3. Права субъекта персональных данных

3.1 Согласие субъекта персональных данных на обработку его персональных данных

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в ФЗ-152, возлагается на Центр.

3.2 Права субъекта персональных данных

Субъект персональных данных имеет право на получение у Центра информации, касающейся обработки его персональных данных, если такое право не ограничено в соответствии с федеральными законами. Субъект персональных данных вправе требовать от Центра уточнения его 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, а также принимать предусмотренные законом меры по защите своих прав.

Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта

персональных данных, если Центр не докажет, что такое согласие было получено.

Центр обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в вышеуказанных целях.

Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных федеральными законами, или при наличии согласия в письменной форме субъекта персональных данных.

Если субъект персональных данных считает, что Центр осуществляет обработку его персональных данных с нарушением требований ФЗ-152 или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в Уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Субъект персональных данных имеет право:

- Требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- 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.
- Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

4. Права оператора персональных данных

Центр вправе:

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

5. Обеспечение безопасности персональных данных

5.1 Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

- Отчета о результатах проведения внутренней проверки;
- Перечня персональных данных, подлежащих защите;
- Акта классификации информационной системы персональных данных;
- Модели угроз безопасности персональных данных;
- Положения о разграничении прав доступа к обрабатываемым персональным данным;
- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Центра. На основании анализа актуальных угроз безопасности ПДн описанного в «Модели угроз» и «Отчета о результатах проведения внутренней проверке», делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в «Мерах защиты персональных данных в ИСПДн».

Список используемых технических средств отражается в «Мерах защиты персональных данных в ИСПДн». Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены главным врачом Центра или лицом, ответственным за обеспечение защиты ПДн.

5.2 Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Центра, являющиеся пользователями 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 подразделения, 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 ИСПДн.

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

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

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

Сотрудники Центра 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.

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

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

При работе с ПДн в ИСПДн сотрудники Центра обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

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

Сотрудники Центра должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

5.3 Ответственность сотрудников Центра

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

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 УК РФ).

Пользователи ИСПДн 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 сотрудниками Центра – пользователей ИСПДн 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 Положениях о подразделениях Центра, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников Центра.

Начальник отдела МИТиТ

«17» февраля 2015 г. _____/Филатов С.С.

СОГЛАСОВАНО
Заместитель главного врача по организационно-методической работе Заведующий Центром Медицинских информационных технологий

«17» 02 2015 г. _____/Волков А.В.