ПРИЛОЖЕНИЕ 1
к приказу от 01.09 2020 г. №166

ПОЛОЖЕНИЕ
об обработке персональных данных в государственном бюджетном учреждение здравоохранения «Челябинский областной клинический кожно-венерологический диспансер»

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных (далее – Положение) в государственном бюджетном учреждение здравоохранения «Челябинский областной клинический кожно-венерологический диспансер» разработано в соответствии с Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», Федеральным законом «Об основах охраны здоровья граждан в Российской Федерации», Правилами внутреннего трудового распорядка ГБУЗ «ЧОККВД» и другими нормативно-правовыми актами в области обеспечения безопасности персональных данных.
1.2. Цель разработки Положения – определение порядка обработки персональных данных в ГБУЗ «ЧОККВД», обеспечение защиты прав и свобод человека и гражданина, в том числе работника, пациента, субъектов из других медицинских организаций по Челябинской области при обработке их персональных данных в ГБУЗ «ЧОККВД», а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм настоящего законодательства РФ, регулирующих обработку и защиту персональных данных.

2. Основные понятия и сокращения, используемые в данном положении

2.1. Оператор персональных данных (далее 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. В рамках настоящего положения оператором является государственное бюджетное учреждение здравоохранения «Челябинский областной клинический кожно-венерологический диспансер»;
2.2. Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния;
2.3. Медицинская организация – юридическое лицо независимо от организационно-правовой формы, осуществляющее в качестве основного (уставного) вида деятельности медицинскую деятельность на основании лицензии, выданной в порядке, установленном законодательством Российской Федерации.
2.4. Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;
2.5. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
2.6. 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;

2.7. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

2.8. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

2.9. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

2.10. 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;

2.11. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

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

2.13. Лечащий врач – врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения;

2.14. Работник – физическое лицо, вступившее в трудовые отношения с работодателем;

2.15. Работодатель – физическое лицо либо юридическое лицо (организация), вступившее в трудовые отношения с работником.

2.16. Перечень сокращений:

АРМ – автоматизированное рабочее место;

ИСПДн – информационная система персональных данных.

3. Состав персональных данных в ГБУЗ «ЧОККВД»

3.1. Состав персональных данных определен Перечнем персональных данных, обрабатываемых в информационных системах персональных данных ГБУЗ «ЧОККВД».

3.2. Обработка персональных данных ИСПДн «Бухгалтерия и кадры» ведется в следующих отделах:

- отдел кадров;
- бухгалтерия;
- экономический отдел.

3.3. Обработка персональных данных ИСПДн «Медицинская информационная система» ведется в следующих отделах:

- регистратура;
- кабинеты врачей;
- отдел статистки;
- стационар;
- лаборатория.

4. Обработка персональных данных в ГБУЗ «ЧОККВД»

4.1. Обработка персональных данных ИСПДн «Бухгалтерия и кадры»:

4.1.1. Сбор персональных данных осуществляется путем предоставления их самим работником, в том числе персональные данные работников филиалов ГБУЗ «ЧОККВД».

4.1.2. Работодатель не обрабатывает персональные данные работника, относящиеся к специальной категории персональных данных.

4.1.3. Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.
4.1.4. Работники не должны отказываться от своих прав на сохранение и защиту персональных данных.
4.1.5. При поступлении на работу работник предоставляет сотрудникам отдела кадров следующие документы, содержащие персональные данные:

- 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;
- свидетельство о регистрации индивидуального налогового номера (ИНН);
- 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;
- свидетельства о рождении детей и заключении брака.

4.1.6. Персональные данные работников хранятся на электронных носителях, включая:

- АРМ работника отдела кадров;
- АРМ работника бухгалтерии;
- АРМ работника экономического отдела.

4.1.7. Персональные данные работников хранятся на бумажных носителях, включая:

- личную карточку работника;
- трудовой договор;
- трудовую книжку;
- копию паспорта;
- копию документа об образовании;
- копии свидетельств о рождении детей и заключении брака.

4.1.8. Сроки хранения персональных данных данной ИСПДн составляют:

- в течение срока работы работника для бумажных носителей персональных данных;
- в электронном виде персональные данные хранятся до ликвидации ИСПДн.

4.2. Обработка персональных данных ИСПДн «Медицинская информационная система»:
4.2.1. Сбор персональных данных пациента осуществляется как путем предоставления их самим пациентом, так и в ходе медицинской деятельности.
4.2.2. Персональные данные пациента могут быть получены в ходе медицинской деятельности, включая:

- анамнез;
- диагноз;
- вид оказанной медицинской помощи;
- сроки оказания медицинской помощи;
- результат обращения за медицинской помощью;
- сведения об оказанных медицинских услугах.

4.2.3. При записи на прием к врачу пациент предоставляет следующие документы, содержащие персональные данные:

- паспорт или иной документ, удостоверяющий личность, гражданство;
- полис ОМС (при наличии).

4.2.4. Согласие на обработку персональных данных.

4.2.5. Персональные данные пациентов хранятся на сервере ИСПДн «Медицинская информационная система» 454113, Челябинская область, г. Челябинск, пл. Революции, д. 4

4.2.6. Персональные данные пациентов хранятся на бумажных носителях, включая:

- медицинская карта амбулаторного больного;
- медицинская карта стационарного больного;
- статистическая карта выбывшего из стационара;
- больничный лист;
- договор на оказание платных медицинских услуг;
- сертификат об отсутствии ВИЧ-инфекции;
- справка об отсутствии инфекционных заболеваний.

4.2.7. Сроки хранения персональных данных данной ИСПДн составляют:

- в электронном виде персональные данные хранятся до ликвидации ИСПДн;
- 1 год для бумажных носителей информации.

4.3. По истечению срока хранения, носители персональных данных передаются в архив.

4.4. При необходимости уничтожения носителей персональных данных составляются акты: Акт уничтожения бумажных носителей персональных данных (Приложение 1) и Акт уничтожения электронных носителей персональных данных (Приложение 2).

5. Доступ к персональным данным в ГБУЗ «ЧОККВД»

5.1. Внутренний доступ (доступ внутри ГБУЗ «ЧОККВД»):

5.1.1. Право доступа к персональным данным ИСПДн «Бухгалтерия и кадры» имеют:

- главный врач ГБУЗ «ЧОККВД»;
- сотрудники отдела кадров;
- сотрудники бухгалтерии;
- сотрудники экономического отдела;
- сам работник.

5.1.2. Право доступа к персональным данным ИСПДн «Медицинская информационная система» имеют:

- главный врач ГБУЗ «ЧОККВД»;
- лечащий врач пациента;
- сотрудники регистратуры;
- статистик;
- сам пациент.

5.2. Субъект персональных данных имеет право:

- Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные субъекта, если это право не ограничено федеральными законами РФ;
- Требовать от ГБУЗ «ЧОККВД» уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для ГБУЗ «ЧОККВД» персональных данных.
-

6. Передача персональных данных в ГБУЗ «ЧОККВД»

6.1. Передача персональных данных в ИСПДн «Бухгалтерия и кадры»:

6.1.1. В целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получения образования и продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, возможна передача персональных данных работника в:

- Пенсионный фонд;

- Федеральную налоговую службу;
- военный комиссариат;
- банковские организации.

6.1.2. Персональные данные, передаваемые в Пенсионный фонд:

- ФИО;
- пол;
- дата рождения;
- адрес прописки и адрес проживания;
- данные паспорта;
- страховое свидетельство государственного пенсионного страхования (СНИЛС);
- период трудовой деятельности и трудовой стаж;
- сведения об окладе.

6.1.3. Персональные данные, передаваемые в Федеральную налоговую службу:

- ФИО;
- пол;
- дата рождения;
- адрес прописки и адрес проживания;
- данные паспорта.
- свидетельство о регистрации индивидуального налогового номера (ИНН).

6.1.4. Персональные данные, передаваемые в военный комиссариат:

- ФИО;
- пол;
- дата рождения;
- адрес прописки и адрес проживания;
- сведения о семейном положении и составе семьи;
- период трудовой деятельности и трудовой стаж;
- сведения воинского учета.

6.1.5. Персональные данные, передаваемые в банковские организации:

- ФИО;
- свидетельство о регистрации индивидуального налогового номера (ИНН).
- адрес проживания.

6.2. Передача персональных данных в ИСПДн «Медицинская информационная система»:

6.2.1. В целях установления медицинского диагноза, медицинских услуг, в том числе для ведения электронной медицинской карты, персональные данные пациента передаются на сервер МИС «БАРС», Территориальному фонду обязательного медицинского страхования Челябинской области и Министерству здравоохранения Челябинской области, включая:

- паспортные данные;
- данные полиса ОМС.
- анамнез;
- диагноз;
- вид оказанной медицинской помощи;
- сроки оказания медицинской помощи;
- результат обращения за медицинской помощью;

- сведения об оказанных медицинских услугах.

6.3. ГБУЗ «ЧОККВД» не вправе передавать персональные данные третьей стороне без письменного согласия субъекта за исключением следующих случаев:

- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

- обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг;

- по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора, 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;

- при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

- в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

- в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти;

- в целях осуществления учета и контроля в системе обязательного социального страхования;

- в целях осуществления контроля качества и безопасности медицинской деятельности.

6.4. Предупреждать лиц, получающих персональные данные субъекта, что они могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

6.5. Разрешать доступ к персональным данным субъектов только лицам, доступ которых к персональным данным, обрабатываемых в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей, при этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения конкретных функций.

6.6. Передача персональных данных вне ГБУЗ «ЧОККВД» должна осуществлять только по защищенным криптографическими методами каналам.

7. Обеспечение безопасности персональных данных

7.1. Обеспечение безопасности персональных данных достигается, в частности:

7.1.1. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

7.1.2. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

7.1.3. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

7.1.4. Обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7.1.5. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;
7.1.6. Учетом машинных носителей персональных данных;
7.1.7. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
7.1.8. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
7.1.9. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.
7.2. Контроль за установленным режимом безопасности персональных данных в ГБУЗ «ЧОККВД» осуществляют ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных.

8. Обязанности работников

8.1. Работник ГБУЗ «ЧОККВД», осуществляющий обработку персональных данных обязан:

- знать и соблюдать установленные требования по условиями и порядку обработки персональных данных, в том числе требования настоящей инструкции;
- работать только с теми документами, содержащими персональными данными, доступ к которым необходим для выполнения работником служебных (трудовых) обязанностей;
- хранить в тайне ставшие известными им сведения, содержащие персональные данные, информировать ответственного за обеспечение безопасности персональных данных о фактах нарушения порядка обращения с персональными данными и о попытках несанкционированного доступа к ним;
- уведомлять ответственного за организацию обработки персональных данных о допущенных нарушениях установленного режима безопасности персональных данных, а также о фактах разглашения сведений, содержащих персональные данные или утрате носителей персональных данных.

8.2. При работе со персональными данными запрещается:

- допускать на свое рабочее место посторонних лиц, а также работников, доступ которых к персональным данным не необходим для выполнения ими должностных обязанностей;
- работать на АРМ, не предназначенном для обработки персональных данных;
- передавать документы, содержащие персональные данные, по открытым каналам связи;
- передавать персональные данные в организации, нерегламентированные настоящим положением и должностными обязанностями;
- использовать сведения, содержащие персональные данные, с неслужебных целях, в разговоре с лицами, не имеющими отношения к этим сведениям;
- отключать или блокировать средства антивирусной защиты информации;
- привлекать посторонних лиц для ремонта или настройки своего АРМ.

8.3. Порядок работы с машинными носителями информации:
8.3.1. Допускается использование только учтенных носителей информации.
8.3.2. Выдача учтенных носителей информации осуществляется только работникам, доступ которых к персональным данным, обрабатываемых в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

8.3.3. Не допускается одновременное наличие данных из разных ИСПДн на одном носителе информации.

8.3.4. При работе с машинными носителями информации запрещается:

- передавать носители третьим лицам;
- хранить носители в неотведенных для этого местах;
- оставлять без присмотра на рабочих столах;
- выносить носители за пределы ГБУЗ «ЧОККВД».

8.3.5. Допускается использование носителей только в рабочих целях.

8.3.6. При потере или краже носителей информации немедленно сообщить об этом ответственному лицу за обеспечение безопасности персональных данных информационной системе или иному лицу, исполняющему его обязанности.

8.3.7. При работе с машинными носителями информации необходимо:

- обеспечить физическую безопасность носителей информации;
- перед работой с носителем провести проверку на наличие вредоносного программного обеспечения;
- бережно относиться к носителям информации;
- по окончанию работы с носителем сдать его на хранение ответственному за обеспечение безопасности персональных данных в информационной системе;

9. Ответственность за нарушение норм, регламентирующих обработку персональных данных

9.1. В соответствии с Федеральным законом 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.

9.2. В УК РФ содержатся следующие статьи, предъявляющие требования по обеспечению безопасной работы с защищаемой информацией (в том числе персональные данные):

9.2.1. Статья 272. Неправомерный доступ к компьютерной информации. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации наказываются штрафом до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на срок до семи лет.

9.2.2. Статья 273. Создание, использование и распространение компьютерных программ. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации наказывается ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на срок до семи лет.

9.2.3. Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации наказывается штрафов в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо принудительными работами на срок до пяти лет, либо ограничением свободы на тот же срок.

9.3. В соответствии со статьями КоАП РФ, нарушение которых ведет к наложению административного штрафа:

9.3.1. Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных). Нарушение влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей.

9.3.2. Статья 13.14. Разглашение информации с ограниченным доступом. Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц – от четырех тысяч до пяти тысяч рублей.