УТВЕРЖДЕНО

Главный врач

Алексеев Г.В.

от «14» 11 2014 г.

№ 25

ПОЛОЖЕНИЕ

по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в Единой государственной информационной системе «Электронное здравоохранение Республики Татарстан»

Бавлы 2014

СОДЕРЖАНИЕ

Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими нормативными правовыми актами Российской Федерации, регулирующими отношения в области защиты персональных данных.

Настоящее Положение вступает в силу с момента подписания приказа об утверждении настоящего Положения руководством Организации.

Настоящее Положение является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным субъектов, а также при проведении работ по защите персональных данных субъектов.

Все сотрудники должны быть ознакомлены с настоящим Положением под роспись. Форма журнала ознакомления с Положением приведена в Приложении 1.

ОСНОВНЫЕ ОПЕРАЦИИ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Обработка персональных данных субъектов осуществляется исключительно с целью оказания медицинских услуг, контроля количества и качества выполняемой работы и обеспечения финансовых расчетов за оказанные услуги в соответствии законами и иными нормативно-правовыми актами.

Под обработкой персональных данных понимается 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.

К обработке, передаче и хранению персональных данных субъекта могут иметь доступ сотрудники, определенные документом «Список лиц, допущенных к работе с персональными данными», утвержденным руководителем Организации.

Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

В состав персональных данных субъектов входят сведения, указанные в документе «Перечень персональных данных, подлежащих защите», утвержденном руководителем Организации.

Получение персональных данных субъектов

При получении персональных данных в информационную систему вводятся сведения об источнике персональных данных и должно быть получено согласие субъекта персональных данных на их обработку.

Персональные данные следует получать у самого субъекта персональных данных. Если персональные данные субъекта возможно получить только у третьей стороны, субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено согласие.

Сотрудники, осуществляющие получение персональных данных субъектов, должны сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

Письменное согласие субъекта на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

Форма письменного согласия субъекта на обработку персональных данных приведена в Приложении 2.

Операторы получают персональные данные непосредственно у субъекта персональных данных или у третьей стороны.

При получении персональных данных непосредственно у субъектов персональных данных операторы должны обеспечить условия, не допускающие необоснованного раскрытия персональных данных третьим лицам, в том числе:

– не должны произноситься персональные данные вслух при заполнении типовых форм, вводе данных в ЕГИС ЭЗРТ, проверке достоверности предоставленных субъектом сведений на основании документов, удостоверяющих личность;

– все некорректно заполненные типовые формы должны быть гарантированно уничтожены;

– не должны оставлять заполненные типовые формы на рабочих столах, а также при приеме третьих лиц.

При получении персональных данных операторы должны руководствоваться документами «Режим обработки персональных данных», «Регламент передачи персональных данных третьим лицам», «Регламент выгрузки и передачи персональных данных».

Хранение, резервное копирование персональных данных субъектов

Хранение персональных данных осуществляется только в серверном сегменте ЕГИС ЭЗРТ.

Подразделение, хранящее персональные данные, обеспечивает их защиту от несанкционированного доступа и копирования согласно настоящему Положению и в соответствии с Постановлением Правительства от 1

ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказа ФСТЭК от 18 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Резервное копирование персональных данных производится в серверном сегменте посредством использования средства EMC Networker. Резервное копирование производится в автоматическом режиме еженедельно каждый понедельник в 00:00. Проверку осуществления резервного копирования осуществляет администратор безопасности.

Уничтожение персональных данных субъектов

Вопросы уничтожения персональных данных субъектов, в том числе на бумажных и электронных носителях, возложены на Комиссию по обеспечению безопасности персональных данных, утвержденную Приказом _____№ __ от «__» _____ 20__ года.

Персональные данные субъектов подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных необходимо прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с момента поступления указанного отзыва.

Уничтожение персональных данных сопровождается составлением акта уничтожения персональных данных. Форма Акта об уничтожении персональных данных, находящихся на электронных носителях приведена в Приложении 3.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ

Защита персональных данных субъектов представляет собой регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности.

Целью несанкционированного доступа к информационным ресурсам является следующее:

- овладение ценными сведениями и их использование;
- видоизменение сведений;
- уничтожение сведений;
- подмена сведений;
- фальсификация содержания реквизитов документа и др.

Посторонним лицам запрещен доступ в помещения, в которых проходит обработка персональных данных субъектов. Порядок доступа к персональным данным описан в документе «Положение о разграничении доступа к Единой государственной информационной системе «Электронное здравоохранение Республики Татарстан».

В целях обеспечения физической защиты персональных данных субъектов необходимо учитывать следующее:

- порядок приема, учета и контроля деятельности посетителей;
- организация и контроль пропускного режима;
- учет и порядок выдачи пропусков;
- технические средства охраны, сигнализация;

– порядок охраны территории, зданий, помещений, транспортных средств.

Для обеспечения технической защиты персональных данных субъектов необходима реализация следующих средств защиты:

– применение сертифицированных СЗИ;
– использование сертифицированных МЭ не ниже третьего уровня защищенности;
– применение шифрования данных с применением алгоритма шифрования ГОСТ;
– использование средств анализа защищенности системы;
– применение средств антивирусной защиты;
– применение средств контроля целостности;
– использование криптосредств при передаче информации между средствами обработки ПДн;
– использование средств резервного копирования;
– использование систем бесперебойного питания;
– документальный запрет акустической обработки ПДн.

Для исключения возможности реализации угрозы несанкционированного доступа к информации в ЕГИС ЭЗРТ следует принять следующие организационные мероприятия:

– определение порядка доступа к защищаемой информации в ЕГИС ЭЗРТ и техническим средствам ее сбора и обработки;
– разработка и оформление правил пересмотра частной модели угроз;
– определение порядка проведения контрольных мероприятий в ЕГИС ЭЗРТ;
– разработка порядка пропускного режима на объекты, где осуществляется работа с ПДн.

Защита персональных данных субъектов на электронных носителях обеспечивается следующими мерами:

- регистрация и поэкземплярный учет используемых электронных носителей персональных данных субъектов. Форма Журнала учета электронных носителей персональных данных субъектов приведена в Приложении 4;
- обеспечение контроля доступа в помещения, в которых хранятся электронные носители ПДн субъектов;
- учет лиц, допущенных к работе с электронными носителями ПДн субъектов.;
- проведение разбирательств и составление заключений по фактам нарушения условий хранения электронных носителей ПДн субъектов.

Данные мероприятия возлагаются на Комиссию по обеспечению безопасности ПДн.

ОТВЕТСТВЕННОСТЬ ЛИЦ, РАБОТАЮЩИХ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ СУБЪЕКТОВ

Руководитель несет персональную ответственность за определение минимально необходимых для исполнения служебных обязанностей прав доступа Пользователей к ПДн в соответствии с законодательством Российской Федерации.

За нарушение норм, регулирующих получение, обработку и защиту ПДн субъекта, Оператор несет административную ответственность согласно Кодексу об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные субъекта.

Каждый сотрудник, получающий доступ к ПДн, несет единоличную ответственность за сохранность и конфиденциальность информации.

Сотрудники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

В целях защиты своих ПДн, обрабатываемых в ЕГИС ЭЗРТ, субъект имеет право на получение сведений:

- об операторе, о месте нахождения оператора;
- о наличии у оператора ПДн, относящихся к соответствующему субъекту персональных данных;
- на подтверждение факта обработки ПДн оператором, а также цели такой обработки;
- о способах обработки ПДн, применяемые оператором;
- о лицах, которые имеют доступ к ПДн или которым может быть предоставлен такой доступ;
- о перечне обрабатываемых ПДн и источник их получения;
- о сроках обработки ПДн, в том числе сроки их хранения;
- о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его ПДн.
- на ознакомление с ПДн, за исключением случая, когда предоставление ПДн нарушает конституционные права и свободы других лиц;
- принимать предусмотренные законом меры по защите своих прав.

Субъект ПДн в праве требовать от оператора уточнения своих ПДн, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

Субъект ПДн обязан передавать достоверные ПДн.

ПОРЯДОК ПЕРЕСМОТРА ПОЛОЖЕНИЯ

Настоящее Положение подлежит пересмотру с целью его актуализации в плановом порядке.

Изменения в настоящее Положение могут быть внесены как по результатам планового пересмотра Положения, так и по инициативе руководителей подразделений или руководства Организации.

Все изменения в Положение вносятся приказом руководителя Организации.

ПРИЛОЖЕНИЕ 1

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ЕГИС ЭЗРТ

ЖУРНАЛ

ознакомления с документом «Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в Единой государственной информационной системе «Электронное здравоохранение Республики Татарстан»

№ п/п	Ф.И.О.	Наименование подразделения	Должность	Дата	Ознакомлен (подпись)
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

ПРИЛОЖЕНИЕ 2

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ЕГИС ЭЗРТ

Руководителю _____

(Наименование организации)

_____

(Ф.И.О. руководителя)

от _____

(Ф.И.О. заявителя, должность)

ЗАЯВЛЕНИЕ

о согласии на обработку персональных данных

Я, _____,

(Ф.И.О. заявителя полностью)

зарегистрированный по адресу: _____,

проживающий по адресу: _____,

паспорт гражданина РФ серии _____№_____, выдан

_____

подтверждаю свое согласие на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно:

- фамилия, имя отчество;
- дата рождения;
- пол;
- адрес места жительства (по паспорту и фактический);
- данные паспорта (свидетельства о рождении);

- место работы (учебы) и должность;
- статус СНИЛС;
- полис ОМС;
- группа инвалидности, группа здоровья;
- сведения о состоянии здоровья (заболевания в текущем году, клинико-статическая группа, листок нетрудоспособности, дата обследования на RW, ВИЧ);
- сведения о пребывании в ЛПУ (причина госпитализации, дата поступления в стационар, отделение, дата выписки, основное заболевание) , –

в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг.

В процессе обработки персональных данных предоставляю оператору право осуществлять следующий перечень действий с моими персональными данными:

- обработку (сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение) моих персональных данных неавтоматизированным способом;
- обработку (сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение) моих персональных данных автоматизированным способом;
- обмен (прием и передача) моих персональных данных со страховой медицинской организацией и территориальным фондом обязательного медицинского страхования, с использованием машинных носителей или по каналам связи с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа;
- передачу моих персональных данных другим должностным лицам Учреждения-оператора с использованием бумажных и машинных

носителей, в том числе по каналам связи и по внутренней сети организации с использованием технических и программных средств защиты информации;

- передачу моих персональных данных следующим третьим лицам:
  - Центр информационных технологий Республики Татарстан
    Адрес оператора: Казань, Петербургская, д.52
    ОГРН: 1091690014712
  - Министерство здравоохранения Республики Татарстан
    Адрес оператора: г. Казань, ул. Островского, 11/6
    ОГРН: 1021602841402

В иных случаях оператор обязуется не предоставлять мои персональные данные третьим лицам без моего согласия на то, выраженного в письменном виде.

Настоящее согласие действует до достижения цели обработки персональных данных или момента утраты необходимости в их достижении, если иное не предусмотрено федеральными законами.

Данное согласие считается отозванным с даты получения оператором письменного уведомления от меня об отзыве настоящего согласия.

В случае изменения сведений, предоставленных мной оператору в соответствии с настоящим согласием, обязуюсь предоставлять оператору актуальные сведения в течение пяти рабочих дней с момента изменения таких сведений.

Об ответственности за достоверность представленных сведений предупрежден.

_____/_____/
(подпись заявителя) (расшифровка подписи)

«_____» _____ 201___г.

ПРИЛОЖЕНИЕ 3

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ЕГИС ЭЗРТ

АКТ № ____

об уничтожении персональных данных, находящихся на электронных носителях

г. Казань «___» _____20__г.

На основании документа «Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в Единой государственной информационной системе «Электронное здравоохранение Республики Татарстан», утвержденного Приказом _____ №_____ от «_____» _____ 20__г. Комиссией по обеспечению безопасности персональных данных в составе:

Председатель комиссии:

_____ _____

(должность) *(Фамилия, И.О.)*

Члены комиссии:

_____ _____

_____ _____

_____ _____

_____ _____

составлен настоящий акт в том, что «____»_____20___г. произведено уничтожение персональных данных субъектов:

№ п п	Наименование носителя	ФИО ответственного пользователя	Учетный номер носителя	Тип удаляемой информации	Способ удаления	Причина удаления[1]

Председатель комиссии:

_____ _____ _____

(должность) *(подпись)* *(Фамилия, И.О.)*

Члены комиссии:

_____ ____ _____ _____

_____ ____ _____ _____

_____ ____ _____ _____

_____ ____ _____ _____

[1] Возможные причины удаления информации с носителя:
1. выявлением неправомерной обработки персональных данных;
2. подтверждением факта неточности персональных данных;
3. выявлением неправомерности обработки персональных данных;
4. достижением цели обработки персональных данных;
5. отзывом субъектом персональных данных согласия на обработку персональных данных.

ПРИЛОЖЕНИЕ 4

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ЕГИС ЭЗРТ

ЖУРНАЛ

учета электронных носителей персональных данных субъектов

№ п/п	Регистрационный номер носителя	Наименование носителя	Категория информации	Дата выдачи	ФИО, должность ответственного пользователя	Подпись получателя	Дата возврата	Подпись ответственного за учет носителей
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

ПРИЛОЖЕНИЕ 5

к Положению по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в ЕГИС ЭЗРТ

Руководителю _____

(Наименование организации)

_____

(Ф.И.О. руководителя)

от _____

(Ф.И.О. заявителя, должность)

ЗАЯВЛЕНИЕ

об отзыве согласия на обработку персональных данных

Настоящим заявлением отзываю свое согласие на обработку персональных данных.

Прошу в срок, не превышающий трех рабочих дней с даты поступления настоящего отзыва, прекратить обработку моих персональных данных (в том числе у лиц, кому эта информация была передана) и направить в мой адрес уведомление о прекращении обработки персональных данных и их уничтожении (удалении из базы данных).

_____/_____ /

(подпись заявителя) (расшифровка подписи)

«_____» _____ 201___г.