

УТВЕРЖДАЮ

Генеральный директор
ОАО «Новая Поликлиника-
Астрахань»

 Сидоров Г.А.

«__» _____ 20__ г.

ПОЛОЖЕНИЕ

о разрешительной системе допуска к информационным ресурсам
ОАО «Новая Поликлиника-Астрахань»

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 №152-ФЗ, постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и другими нормативными документами.

1.2. Разрешительная система допуска к информационным ресурсам ОАО «Новая Поликлиника-Астрахань» (далее- Поликлиника) представляет собой совокупность процедур оформления права субъектов на доступ к информационным ресурсам (объекты доступа) организации и ответственных лиц, осуществляющих реализацию этих процедур.

1.3. Объектами доступа являются:

- документированная информация на бумажных носителях в виде отдельных документов или дел;
- информационные ресурсы в информационной системе в виде баз данных, библиотек, архивов и их копий на машинных носителях.

1.4. Субъектами доступа являются:

- работники Поликлиники;
- юридические и физические лица.

1.5. Субъекты доступа несут персональную ответственность за соблюдение ими установленного в поликлинике порядка обеспечения защиты информационных ресурсов.

1.6. Ответственными лицами Поликлиники, осуществляющими реализацию процедур оформления прав субъектов на доступ к информационным ресурсам, являются:

- руководитель;
- заместители руководителя;
- начальники отделов;
- администратор (безопасности) ИСПДн;
- ответственный за защиту информации.

2. Порядок формирования информационных ресурсов поликлиники

2.1. Формирование информационных ресурсов на бумажных носителях осуществляется в структурных подразделениях и регламентируется инструкцией по делопроизводству организации.

2.2. Информационные ресурсы, формируемые в ИСПДн, подразделяются на:

- сетевые ресурсы с доступом одной группы пользователей (ресурсы отдела);
- сетевые ресурсы с доступом нескольких групп пользователей (базы данных и т.п.);
- ресурсы общего пользования (справочно-информационные системы, библиотеки, каталоги и т.п.);
- сетевой ресурс почтового обмена;
- сетевые принтеры;
- ресурсы пользователя (сетевые или локальные).

2.3. Информационные ресурсы, содержащие персональные данные, указываются в «Перечне информационных ресурсов, содержащих персональные данные, подлежащих защите».

2.4. Решение о формировании новых информационных ресурсов принимает начальник отдела, инициирующего это решение. В заявке на формирование обосновывается необходимость создания новых информационных ресурсов и указывается, в интересах каких групп пользователей они создаются.

2.5. Непосредственное формирование нового сетевого информационного ресурса осуществляется администратором ИСПДн. На исполненной заявке администратор ИСПДн проставляет отметку о создании и местонахождении ресурса.

2.6. На основании исполненной заявки вносятся изменения и дополнения в «Матрицу разграничения доступа к ИСПДн» и «Перечень информационных ресурсов, содержащих персональные данные, подлежащих защите в ИСПДн».

3. Допуск к информационным ресурсам работников поликлиники

3.1. Допуск работников к информации, содержащей персональные данные, осуществляется в соответствии с занимаемой должностью и в объеме, необходимом для выполнения ими должностных обязанностей.

3.2. Допуск к персональным данным разрешается руководителем, только уполномоченным лицам с соблюдением требований Положения об обработке персональных данных (Приложение №10 к приказу № 50/1-А от 27.07.2016г.).

3.3. Допуск работника к информационным ресурсам ИСПДн оформляется заявкой администратору ИСПДн, которая предоставляется начальником соответствующего отдела после согласования с руководителем. В заявке указывается, к каким ресурсам и с какими правами (полномочиями) допустить конкретного работника.

3.4. Администратором безопасности (или ответственным лицом) проверяется соответствие требуемых прав доступа с реально необходимыми для выполнения должностных (функциональных) обязанностей данного работника.

3.5. Согласованная заявка является разрешением на допуск и основанием для регистрации пользователя в сети администратором ИСПДн. Заявки подшиваются и хранятся в отделе информационного обеспечения.

4. Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций поликлиники

4.1. К организациям, деятельность которых не связана с исполнением функций поликлиники, могут относиться:

- правоохранительные органы;
- судебные органы;
- органы статистики;
- органы исполнительной и законодательной власти субъектов Российской Федерации;

- средства массовой информации и пр.

4.2. Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций организации, регламентируется законодательством Российской Федерации, договорами и соглашениями об информационном обмене и другими нормативными актами.

5. Допуск к информационным ресурсам поликлиники сторонних организаций, выполняющих работы в поликлинике на договорной основе

5.1. К организациям, выполняющим работы на договорной основе, могут относиться:

- организации, выполняющие строительные работы и осуществляющие ремонт зданий, систем инженерно-технического обеспечения (отопления, освещения, водоснабжения, канализации, электропитания, кондиционирования и т.п.);
- организации, осуществляющие монтаж и настройку технических средств ИСПДн, сопровождение программно-прикладного обеспечения;
- организации, оказывающие услуги в области защиты информации (проведение специальных проверок и исследований, монтаж и настройка средств защиты информации, контроль эффективности системы защиты информации, аттестация объектов информатизации и т.п.);
- организации, осуществляющие поставку товаров для обеспечения повседневной деятельности (медицинское оборудование, медицинскую мебель и мед.технику, канцтоваров, оргтехники, расходных материалов и т.п.);

5.2. Порядок допуска определяется в договоре на выполнение работ (оказание услуг), в соответствии с «Положением об обработке персональных данных в ОАО «Новая Поликлиника-Астрахань» (Приложение №10 к приказу № 50/1-А от 27.07.2016г).

5.3. Решением о допуске является подписанный в установленном порядке договор на выполнение работ или оказание услуг.

5.4. В договор на оказание услуг включается условие о неразглашении сведений, составляющих персональные данные, а также служебной информации, ставшей известной в ходе выполнения работ, если для их выполнения предусмотрено использование таких сведений. Со всех работников сторонней организации, участвующих в выполнении работ, в этом случае берется подписка о неразглашении таких сведений.

6. Доступ к информационным ресурсам поликлиники

6.1. Правила и процедуры доступа к информационным ресурсам поликлиники определяются об обработке персональных данных в ОАО «Новая Поликлиника-Астрахань» и настоящим Положением.

6.2. Администрирование прав доступа к информации в ИСПДн производится администратором ИСПДн.

6.3. После регистрации пользователя в ИСПДн администратор безопасности ИСПДн вносит изменения в «Матрицу разграничения доступа к ИСПДн» для последующего контроля прав и полномочий пользователя.

6.4. Администратор ИСПДн производит настройку сети в соответствии с требованиями Положения об организации и проведении работ по обеспечению безопасности персональных данных.

7. Контроль функционирования разрешительной системы допуска к информационным ресурсам поликлиники

7.1. Контроль функционирования разрешительной системы допуска к информационным ресурсам организуется в соответствии с:

- планом основных мероприятий по защите информации на текущий год;
- функциональными обязанностями должностных лиц;
- приказами руководителя.

7.2. Контроль функционирования разрешительной системы допуска к информационным ресурсам осуществляется ответственными лицами. Организация контроля возлагается на администратора безопасности.

8. Документальные составляющие

8.1. Список сотрудников, допущенных к обработке персональных данных ведет системный администратор.

8.2. Начальник ИТО формирует матрицу разграничения доступа к информационным ресурсам ИСПДн.

8.3. Перечень информационных ресурсов, содержащих персональные данные, подлежащие защите в ИСПДн» определяет начальник.

8.4. Финансовый директор при заключении договоров на выполнение работ, оказание услуг предусматривает в договоре обязательства сторон о неразглашении сведений.