Приложение № 2
Политики обработки и
защиты персональных данных,
утв. Приказом главного врача
№ 262 от 27.06.2017 г.

УТВЕРЖДАЮ
Главный врач
БУЗ УР «Можгинская РБ МЗ УР»

_____ Н.П. Вдовина

«_27_» _июня_ 2017 год

Перечень
персональных данных, подлежащих защите в информационных системах персональных данных БУЗ УР «Можгинская РБ МЗ УР»

1. Персональные данные субъектов персональных данных (ПДн) (пациентов) включают:
   - Ф.И.О.;
   - Дата рождения;
   - Контактный телефон;
   - Адрес прописки;
   - Адрес фактического проживания;
   - Паспортные данные;
   - № СНИЛС;
   - Полис ОМС;
   - Данные о состоянии здоровья (история болезни).
2. Персональные данные работников Учреждения включают:
   - Ф.И.О.;
   - место, год и дата рождения;
   - адрес по прописке;
   - паспортные данные (серия, номер паспорта, кем и когда выдан, код подразделения)
   - информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
   - информация о трудовой деятельности до приема на работу;
   - информация о трудовом стаже (место работы, должность, период работы, причины увольнения);
   - адрес проживания (фактический);
   - телефонный номер (домашний, рабочий, мобильный);
   - семейное положение и состав семьи (муж/жена, дети);
   - информация о знании иностранных языков;
   - форма допуска;
   - оклад;
   - данные о трудовом договоре (номер трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытания сроком, режим труда, длительность всех видов отпусков, обязанности работника, дополнительные социальные льготы и гарантии, номер и число изменений к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочего времени, система оплаты и т.д.);
   - сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
   - ИНН;
   - данные об аттестации работников;
   - данные о повышении квалификации;

- данные о наградах, медалях, поощрениях, почетных званиях;
- информация о приеме на работу, перемещении, увольнении;
- информация об отпусках;
- информация о командировках;
- информация о болезнях;
- информация о негосударственном пенсионном обеспечении;
- и т.д.

3. Технологическая информация, подлежащая защите, включает:
   - управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
   - технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа,программно-аппаратные и др.);
   - информация на съемных носителях информации (магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
   - информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
   - служебные данные (метаданные), появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки обрабатываемой информации.
4. Программно-технические средства обработки включают в себя:
   - общесистемное и специальное программное обеспечение (операционные системы, системы управления базы данных (СУБД), клиент-серверные приложения и другие);
   - резервные копии общесистемного программного обеспечения;
   - инструментальные средства и утилиты систем управления ресурсами информационной системы персональных данных (ИСПДн);
   - аппаратные средства обработки ПДн (АРМ и сервера);
   - сетевое оборудование (Межсетевой экран, коммутаторы, маршрутизаторы и т.п.).
5. Средства защиты ПДн состоят из аппаратно-программных средств, включают в себя:
   - средства управления и разграничения доступа пользователей;
   - средства, обеспечивающие целостность данных;
   - средства антивирусной защиты;
   - средства межсетевого экранирования;
   - средства обнаружения вторжений;
   - средства криптографической защиты ПДн при их передаче по каналам связи сети общего и (или) международного обмена.
6. Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передается обрабатываемая и технологическая информация.
7. Объекты и помещения являются объектами защиты, если в них происходит обработка, накопление и сбор информации, использующаяся в рабочем процессе, в том числе любая информация, относящаяся к персональным данным.

Приложение № 1
Политики обработки и
защиты персональных данных,
утв. Приказом главного врача
№ 262 от 27.06.2017 г.

УТВЕРЖДАЮ
Главный врач
БУЗ УР «Можгинская РБ МЗ УР»

_____ Н.П. Вдовина

«27» июня 2017 год

Правила
доступа работников БУЗ УР «Можгинская РБ МЗ УР» в помещения, в которых ведется обработка персональных данных

1. Настоящие Правила доступа работников БУЗ УР «Можгинская РБ МЗ УР» (далее – Учреждение) в помещения, в которых ведется обработка персональных данных, разработаны в соответствии с требованиями Федерального закона «О персональных данных» № 152-ФЗ от 27.07.2006 года.
2. В БУЗ УР «Можгинская РБ МЗ УР» персональные данные работников Учреждения и граждан хранятся:
   - в отделе по организационно-методической работе (на бумажных и электронных носителях)
   - в отделах правовой и кадровой работы (на бумажных и электронных носителях)
   - в планово-экономическом отделе (на бумажных и электронных носителях)
   - в отделе бухгалтерского учета (на бумажных и электронных носителях)
   - в отделе учета и медицинской статистики (на бумажных и электронных носителях)
   - в штабе гражданской обороны (на бумажных и электронных носителях)
3. Помещения, в которых ведется обработка персональных данных, должны обеспечивать сохранность информации и технических средств, исключить возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами.
4. Персональные данные на бумажных носителях должны находиться в недоступном для посторонних лиц месте. Бумажные носители персональных данных и электронные носители персональных данных (диски флеш-карты) хранятся в шкафах, оборудованных замками.
5. Помещения, в которых ведется обработка персональных данных, запираются на ключ. Вскрытие и закрытие помещений, в которых ведется обработка персональных данных, производится работниками непосредственно работающими в данном помещении.
6. Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании рабочего дня работники, имеющие право доступа в помещения, обязаны:
   - убрать бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) в шкафы, закрыть шкафы;
   - отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;

- закрыть окна, двери.

7. Перед открытием помещений, в которых ведется обработка персональных данных, работники, имеющие право доступа в помещения, обязаны:
   - провести внешний осмотр с целью установления целостности двери и замка;
   - открыть дверь и осмотреть помещение, проверить наличие и целостность замков на шкафах.
8. При обнаружении неисправности двери и запирающих устройств работники обязаны:
   - не вскрывая помещения, в котором ведется обработка персональных данных, доложить непосредственному руководителю
   - в присутствии не менее двух иных работников, включая непосредственного руководителя, вскрыть помещение и осмотреть его;
   - составить акт о выявленных нарушениях и передать его руководству.
9. Право самостоятельного входа в помещения, где обрабатываются персональные данные, имеют только работники, непосредственно работающие в данном помещении. Иные работники и граждане имеют право пребывать в помещениях, где обрабатываются персональные данные, только в присутствии работников, непосредственно работающих в данных помещениях.
10. При работе с информацией, содержащей персональные данные, двери помещений должны быть всегда закрыты.
11. Техническое обслуживание компьютерной и организационной техники, сопровождение программных средств, уборка помещения, в котором ведется обработка персональных данных, а также проведение других работ осуществляются в присутствии работника, работающего в данном помещении.
12. Ответственность за соблюдение Правил доступа в помещения, в которых ведется обработка персональных данных, возлагается на начальников отделов, обрабатывающих персональные данные.