| | | | |
|---|---|---|---|
| **Наименование структурного подразделения:** | **Все структурные подразделение** | | |
| **Названия документа:** | **СОП "Политика информационной безопасности"** | | |
| **Утвержден:** | Руководитель ГКП на ПХВ «ЛГП»<br>Чалкаров А.Б. | | |
| **Дата утверждения:** | | | |
| **Разработчик:** | *Должность* | *Ф.И.О.* | *Подпись* |
| | Заместитель гл.врача по лечебному делу | Анаркулова У.О. | |
| | Программист | Сопов А.<br>Сухинин А. | |
| | Главная медсестра | Каракулова Д.Т. | |
| **Согласовано:** | Заместитель гл.врача по ОМД | Кабылбеков Г.К. | |
| | Заместитель гл.врача по контролю качества мед.услуг | Рысбаев С.Т. | |
| **Дата согласования:** | 04.01.2024г. | | |
| **Дата введения в действие** | 04.01.2024г. | | |
| **Версия №** | **Копия №_____** | 04 /01 / 2024г.<br>Ф.И.О. _____<br>Подпись _____ | |

Дата последнего пересмотра «04» «01» 2024г
Дата следующего пересмотра «_____» «_____» 2027г

*Запрещается несанкционированное ксерокопирование документа*

## СОП "Политика информационной безопасности"

**1. Цель**

Определить порядок обеспечения информационной безопасности, конфиденциальности информации о пациенте. Целью обеспечения информационной безопасности является минимизация экономического, финансового, социального, институционального и экологического ущерба от реализации угроз информационной безопасности, а также повышение общего уровня конфиденциальности, целостности и доступности информации в информационной системе в ГКП на ПХВ «Ленгерская Городская Поликлиника» (далее –Городская Поликлиника).

**2. Область применения**

1) Политика предназначена для обеспечения информационной безопасности и распространяется на всех работников Городская Поликлиника.

2) Настоящая Политика устанавливает требования к управлению информацией в части обеспечения приватности, конфиденциальности и безопасности информации.

**3. Термины и определения**

В настоящих Правилах применяются следующие определения:

*Медицинская помощь* – комплекс медицинских услуг, направленных на сохранение, укрепление и восстановление здоровья пациента, включающий профилактику, диагностику, лечение, медицинскую реабилитацию и протезирование, осуществляемый медицинскими работниками.

*Управление документами* – комплекс работ по анализу документов на адекватность, учету и поддержанию в рабочем состоянии, распространению и доведению до сведения заинтересованных лиц.

Аутентификация- подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа, реализованных в системе

Авторизация - предоставление прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

Государственные секреты - защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной медицинской, военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права.

4) *Доступность* - состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно

*Запрещается несанкционированное ксерокопирование документа*

5) *Информационная безопасность (далее - ИБ)*- состояние защищенности информационных ресурсов и систем, обеспечение конфиденциальности, целостности и доступности информации.

6) *ИБП* - источник бесперебойного питания

7) *ИС*- информационные системы

8) *Инфраструктура ИС*- каналы связи, оборудование, программное обеспечение, сотрудники и пользователи, документация, информация информационных систем.

9) *Конфиденциальность информации*- обеспечение предоставления информации только авторизированным лицам по уровням доступа

10) *ОМС* - организационно-методическая служба

11) *ОС* - операционная система

12) *ПО* - программное обеспечение

13) *Пользователи ИС*- лица, работающие с ИС

14) *ПП РК*- Постановления Правительства Республики Казахстан

15) *СВТ*- средства вычислительной техники

16) *Целостность информации*- состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право

**4. Ответственность**

1) Специалисты, отвечающие за информационную безопасность ответственность за контроль за выполнением всех пунктов данной Политики. Должен обеспечить четкое управление и зримую поддержку инициатив в области поддержки информационной безопасности информационной системы.

2) Специалисты, отвечающие за информационную безопасность должны обеспечивать координацию мер контроля в эксплуатируемых информационных системах.

3) Специалисты, отвечающие за информационную безопасность должны предоставлять ресурсы для обеспечения мер информационной безопасности.

4) Главврач, и/или лицо назначенное Главврачом должен утверждать распределение специфических ролей и обязанностей по информационной безопасности.

5) Обслуживающий персонал при нарушении требований пунктов Политики информационной безопасности будет привлекаться к административной или иной ответственности, в соответствии с действующим законодательством Республики Казахстан.

6) Специалисты, отвечающие за информационную безопасность должны обеспечить контроль издания и доведения до сведения утвержденных документов по информационной безопасности до обслуживающего персонала и пользователей информационных систем Медицинской организации

*Запрещается несанкционированное ксерокопирование документа*

7) Специалисты, отвечающие за информационную безопасность должны инициировать планы и программы по поддержанию осведомлённости об информационной безопасности.

8) Ответственность на администраторов информационных систем возлагается в соответствии с зонами их ответственности.

9) Администраторы информационных систем обязаны:

a) обеспечивать обязательность процедуры идентификации и аутентификации для доступа к ресурсам информационных систем;

b) не допускать получения права доступа к информационным системам неавторизированным пользователям и представлять пользователям входные имена и начальные пароли только после заполнения установленных регистрационных форм;

c) обеспечивать защиту оборудования, в том числе специальных межсетевых программных средств;

d) оперативно и эффективно реагировать на события, содержащие угрозу, принимать меры по отражению угрозы и выявлению нарушителей, фиксировать и информировать специалистов, отвечающие за информационную безопасность о попытках нарушения защиты.

## 5. Ресурсы

1) Серверное помещение, отвечающее всем требованиям;
2) Источник бесперебойного питания необходимой мощности;
3) Внутренние нормативные документы

## 6. 7. Общие положения

7.1. Настоящая Политика информационной безопасности является внутренним нормативным документом Городской Поликлиники. Политика устанавливает требования к обеспечению Городской Поликлиники, определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих Положений, Правил, Инструкций. Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

Целью обеспечения ИБ является минимизация экономического, финансового, социального, институционального и экологического ущербов от реализации угроз ИБ, а также повышение общего уровня конфиденциальности, целостности и доступности информации в ИС.

7.2. Политика ИБ распространяется на функционирование всей инфраструктуры Городской Поликлиники.

*Запрещается несанкционированное ксерокопирование документа*

7.3. Политика ИБ обязательна для исполнения всеми лицами, работающими с инфраструктурой, в том числе для третьих лиц, выполняющих работы по сопровождению либо развитию ИС.

7.4. Исполнение требований политики ИБ обеспечивают все лица, работающие с инфраструктурой информационных систем.

7.5. Действия по обеспечению ИБ должны координироваться руководством и специалистами, ответственных за ИБ.

7.6. Координация ИБ должна осуществлять следующую деятельность:

a) обеспечивать соответствие выполняемых действий по обеспечению ИБ политике ИБ;

b) определение действий в случае несоответствия выполняемых действий по обеспечению ИБ политике по ИБ;

c) утверждение методологии и процессов обеспечения ИБ, например, оценку рисков, классификацию информации;

d) идентифицировать значительные изменения угроз и подвергание информации и средств обработки информации угрозам;

e) оценивание адекватности и координирования реализации мер контролю ИБ;

f) эффективное способствование обучению, подготовке по ИБ и осведомлённости о ней;

g) оценивание информации, полученной от мониторинга и пересмотра инцидентов ИБ, и внесение рекомендаций в ответ на идентифицированные инциденты ИБ.

## 8. Описание управления информационной безопасностью

### 8.1. Конфиденциальность

1) Главным требованием конфиденциальности является обеспечение предоставления информации только авторизированным лицам.

2) Информация, обрабатываемая и хранящаяся в ИС, подлежит копированию и передаче третьему лицу только с официального разрешения руководства.

3) При работе с ИС должна исключаться возможность наблюдения за отображаемой информацией посторонними лицами.

4) В ИС не должны размещаться документы, содержащие государственные секреты, коммерческую тайну и иную информацию с ограниченным доступом.

5) Запись и копирование служебной и иной защищаемой информации, в том числе для передачи другим лицам, производится на зарегистрированные в установленном порядке носители информации.

6) При работе с ИС должны использоваться специальные лицензионные программные или аппаратные средства, обеспечивающие защиту от вредоносных программ, вирусов и сетевых атак.

*Запрещается несанкционированное ксерокопирование документа*

7) Информация должна классифицироваться с точки зрения ее ценности, правовых требований, секретности и критичности для ИС.

**8.2. Соглашения о конфиденциальности**

1) Требования по соглашениям о конфиденциальности или неразглашении, отражающие потребности по защите безопасности, должны быть определены и регулярно пересмотрены.

a) Для определения требований по соглашениям о конфиденциальности или неразглашении необходимо рассмотреть следующие элементы:

a) определение информации, которая должна быть защищена (т.е. конфиденциальная информация или информация, содержащая коммерческую тайну);

b) предполагаемая продолжительности соглашения, включая случаи, когда конфиденциальность должна поддерживаться бесконечно;

c) требуемые действия по окончанию соглашения;

d) обязанности и действия подписавших сторон во избежание несанкционированного разглашения информации (такого как «принцип необходимого знания»);

e) собственность на информацию, коммерческие секреты и интеллектуальную собственность и то, как она связана с защитой конфиденциальной информации;

f) разрешённое использование конфиденциальной информации и право подписавшей стороны использовать информацию;

g) право аудита и мониторинга действий, в которых задействована конфиденциальная информация;

h) процесс уведомления и сообщения о несанкционированном разглашении или нарушении конфиденциальности информации и коммерческой тайны;

i) условия о возврате или уничтожении информации при прекращении действия соглашения;

j) предполагаемые действия в случае нарушения данного соглашения.

В соглашении о конфиденциальности или неразглашении могут потребоваться дру¬гие элементы, основанные на требованиях безопасности. Соглашения о конфиденциальности и неразглашении должны соответствовать всем применяемым правовым нормам и правилам юрисдикции, которые применяются.

**9. Требования**

**9.1. Требования к обучению и осведомленности в вопросах ИБ**

1) Обслуживающий персонал ИС, пользователи и администраторы ИС, должны быть ознакомлены с политикой ИБ.

2) Обслуживающий персонал ИС должен предоставить пользователям ИС рабочую документацию (Инструкция о парольной защите ИС).

*Запрещается несанкционированное ксерокопирование документа*

3) Обслуживающий персонал ИС по запросу пользователей должен проводить первичный инструктаж по ИБ.

4) Обслуживающий персонал, обеспечивающий функционирование ИС должен проходить регулярно инструктаж по соблюдению ИБ.

5) Обслуживающий персонал ИС должны принять пользовательское соглашение о конфиденциальности.

6) В целях обеспечения ИБ необходимо согласовать и определить в соглашении с третьей стороной мероприятия по управлению ИС.

7) В целях обеспечения гарантированного уведомления подразделения ответственного за ИБ, обслуживающего персонала ИС и всех заинтересованных сторон об инциденте и слабости ИБ по отношению к ИС должны быть реализованы формальные процедуры по уведомлению об инциденте и появлении угроз. Для трансляции уведомлений должен быть избран способ, гарантированно позволяющий своевременно принять корректирующие меры.

8) В рамках работ осуществляется обучение новых сотрудников в работе ИС, разъясняется функция копирования и вставки информации в электронную медицинскую карту и стратегиям и тактикам, применяемым для планового и внепланового простоя ИС.

9) Обслуживающий персонал ИС должен знать процедуры уведомления, а также располагать сведениями о различных типах событий или слабых местах, которые могут влиять на безопасность ресурсов, и о наступлении которых или предпосылках к таковому необходимо отправить уведомление.

10) Обслуживающий персонал и администраторы ИС обязаны как можно быстрее сообщать о любых событиях в сфере ИБ ответственным за ИБ лицам.

### 9.2. Требования по аутентификации ИС

Администраторы и пользователи ИС должны проходить безопасную аутентификацию, идентифицирующую их и исключающую возможность подбора пароля и перехвата авторотационных данных.

### 9.3. Требования к пользовательским учетным записям и паролям

Требования к пользовательским учетным записям и паролям приведены во внутреннем нормативном документе «Инструкция о парольной защите ИС».

### 9.4. Контроль обеспечения конфиденциальности

С целью контроля обеспечения конфиденциальности должны обеспечиваться следующие мероприятия:

a) ежегодный анализ ИБ ИС на соблюдение требований ИБ, с результатом в виде отчета.

b) постоянный мониторинг инструментальными средствами ИБ серверов ИС и сети, в которой они находятся.

*Запрещается несанкционированное ксерокопирование документа*

c) обеспечение предоставления информации авторизированным лицам.

d) подключение пользователей ИС должны строго фиксироваться с сохранением данной информации.

e) информация, обрабатываемая и хранящиеся в ИС, подлежит копированию и передаче третьим лицам только с официального разрешения руководства.

f) при работе с ИС должна исключаться возможность наблюдения за отображаемой информацией третьими лицами.

g) в ИС не должны размещаться документы, содержащие государственные секреты и информацию с ограниченным доступом.

h) электронные истории болезни, электронные амбулаторные карты, результаты инструментальной диагностики и лабораторных исследований, хранящиеся в ИС, не подлежат копированию и передаче третьим лицам, только по запросу уполномоченного органа или иное предусмотренное законом Республики Казахстан.

i) при работе с ИС должны использоваться лицензионные программные или аппаратные средства, обеспечивающие защиту от вредоносных программ, вирусов и сетевых атак.

j) информация должна классифицироваться с точки зрения ее ценности, правовых требований, секретности и критичности для ИС Городской Поликлиники.

### 9.5. Целостность

1) Главным требованием целостности является обеспечение изменения информации только авторизированными лицами по уровням доступа.

2) Новые программно-аппаратные средства, внедряемые должны быть соответствующим образом одобрены со стороны руководства и специалистов, ответственных за обеспечение ИБ.

3) Аппаратные средства и программное обеспечение перед внедрением следует проверять на совместимость с другими компонентами системы.

### 9.6. Требования к антивирусной безопасности

Требования к антивирусной защите приведены во внутреннем нормативном документе «Инструкция по организации антивирусной защиты».

### 9.7. Требования к применению электронной почты и Интернета

Требования по использованию электронной почты и Интернета приведены во внутреннем нормативном документе «Инструкция по использованию электронной почты и служб Интернет на подстанциях».

### 9.8. Доступность

*Запрещается несанкционированное ксерокопирование документа*

1) Главным требованием доступности является обеспечение состояния информации (ресурсов автоматизированной информационной системы), при котором авторизированные лица могут работать с ней беспрепятственно.

2) В случае возникновения внештатных ситуаций, аварий, стихийных бедствий и иных ситуаций, которые могут повлиять, должны быть предусмотрены соответствующие меры защиты и обеспечения непрерывной работы и восстановления.

3) Аварии, стихийные бедствия и иные внештатные ситуации должны фиксироваться в полном и тщательном виде, с сохранением данной информации на срок не менее 2-х лет.

4) В случае возникновения инцидента ИБ или другой нештатной ситуации необходимо руководствоваться «Инструкцией о порядке действий пользователей во внештатных (кризисных) ситуациях».

### 9.9. Требования по бесперебойному питанию

Бесперебойное электропитание обеспечивается ИБП (источником бесперебойного питания) необходимой мощности, который должен гарантировать, как минимум, корректное завершение работы приложений и сворачивание операционной системы при отключении внешнего электропитания.

### 9.10. Требования по обеспечению резервирования и дублирования мощностей

1) Система хранения данных должна предусматривать автоматический периодический контроль целостности дисков, анализ плохих секторов, проверку состояния резервных батарей, без вмешательства администратора и без влияния на работу пользователей.

2) Система хранения данных должна обеспечивать возможность «горячей» замены дисков.

### 9.11. Требования по обеспечению оперативного мониторинга состояния доступности

Мониторинг ИС производится ежедневно в течение рабочего дня с помощью специализированного программного обеспечения, в случае изменения состояния доступности ИС произойдет оповещение администратора в режиме «онлайн».

### 9.12. Управление инцидентами и несоответствиями требованиям ИБ

Кроме сообщений о случаях нарушения и слабых местах ИБ для обнаружения инцидентов нарушения ИБ должен применяться мониторинг систем, предупреждений и уязвимостей. Для процедур управления инцидентами нарушения ИБ должны рассматри¬ваться следующие правила:

*Запрещается несанкционированное ксерокопирование документа*

1) Для работы с различными типами инцидентов необходимо установить следующие процедуры:

a) сбои информационных систем и утрата сервисов;
b) вредоносный код;
c) отказ в обслуживании;
d) ошибки вследствие неполных или неточных данных;
e) нарушения конфиденциальности и целостности;
f) неправильное использование информационных систем;

2) Дополнение к обычным планам обеспечения непрерывности должны существовать процедуры касательно:

a) анализа и идентификации причины инцидента;
b) локализации;
c) планирования и внедрения средств, предотвращающих повторное проявление
d) инцидентов, при необходимости;
h) сообщённым инцидентам ИБ;
i) рекомендациям, представленным соответствующими учреждениями.

4) Политика ИБ должна пересматриваться в случае появления существенных изменений в целях обеспечения конфиденциальности, целостности, доступности.

### 9.16 Контроль на соответствие требованиям ИБ

Контроль требований настоящей политики ИБ осуществляют специалисты, отвечающие за ИБ.

## 10. Документирование

Ежегодный анализ информационной безопасности информационных систем с результатом в виде отчет

## 11.Указание условий пересмотра СОП:

Пересмотр СОП проводиться 1 раз в 3 года или при появлении новых требовании.

*Приложение 1*

### Оценка возможных технических рисков

| Вид риска | Описание | Измерения и меры по снижению риска |
|---|---|---|
| Выход из строя сервера | Сбой в работе аппаратного или ПО сервера. | Измеряется в процентной доле времени штатного функционирования. Предусматривать длительный срок гарантийного обслуживания при |

| Вид риска | Описание | Измерения и меры по снижению риска |
|---|---|---|
| | | заключении договора, а по его окончании - резервирование серверов |
| Выход из строя рабочей станции | Сбой в работе аппаратного или ПО рабочей станции. | Измеряется в процентной доле времени штатного функционирования. Приобретение только у ведущих мировых производителей, имеющих сертифицированные сервис центры |
| Потеря или искажение данных при передаче | Частичная потеря или искажение данных при передаче по каналам связи из-за сбоев в телекоммуникационном оборудовании с учетом корректирующих свойств коммуникационных протоколов. | Измеряется в доле потерянных либо искаженных данных. Перевод на наземные каналы связи и резервирование каналов |
| Потеря или искажение данных при хранении | Риск вызван возможностью сбоев в файловой системе диска или физическими ошибками на накопителях, с учетом способа хранения данных в БД. | Измеряется в среднем времени между отказами в часах. Наращивание систем хранения информации, периодическое резервное копирование согласно инструкции. |
| Быстрое моральное устаревание технологий | Неприятие ППО пользователями | Уточнение требований заявителя по платформенной независимости ППО |
| Приобретение морально-устаревшей техники | Отсутствие комплектующих материалов<br>Отсутствие технической поддержки морально- | Уточнение требований заявителя составлением детальных технических спецификаций на работы при подписании договоров с Поставщиками услуг |

*Запрещается несанкционированное ксерокопирование документа*

| Вид риска | Описание | Измерения и меры по снижению риска |
|---|---|---|
| | устаревшего оборудования | |
| Снижение ИБ | Внешнее воздействие на информационные сети, в том числе атаки хакеров и компьютерных вирусов | Мониторинг и аудит системы обеспечения ИБ. Осуществление анализа эффективности принятых мер по защите информации с учетом изменений ИКТ-среды, появление новых угроз, инцидентов и проблем. Внедрение дополнительных мер защиты |

**Уровни защиты и доступа к информации**

Определены три уровня защиты и доступа к информации:

1) **конфиденциальный** – к данному уровню относится коммерческая и служебная тайна. Также сюда относятся медицинские карты пациентов. Распространение сведений из медицинской карты пациента для лиц, не оказывающих лечение, уход или аудит, разрешено устного с разрешения пациента, если для публикации – то с письменного разрешения пациента; Доступ в серверные помещения только определенно установленным сотрудникам;

2) **ограниченный** – к данному уровню относится информация, не отнесенная к категории «конфиденциальная», разглашение которой может потенциально нанести ущерб интересам организации. Например: переписка с внешними организациями, протоколы совещаний, внутренние правила и процедуры, служебные записки, личные дела сотрудников и др. Доступ к таким документам имеет адресат или лицо, имеющее право доступа для выполнения им должностных обязанностей согласно Должностной инструкции работника;

3) **открытый (неограниченный)** – к данному уровню относится информация, обеспечение конфиденциальности (введения ограничений на распространение) которой не требуется. Например: памятки для пациентов, прейскурант цен на оказываемые услуги и т.п.

**Сохранение и уничтожение документов**

1) Оригинал отмененного (недействительного) документа хранится в Канцелярии **в течение 5 лет.** На оригинале отмененного документа ставится надпись «Признан утратившим силу, согласно_№_от_» и подпись сотрудника Канцелярии.

2) Срок хранения иных документов (медицинской карты и т.п.) определяется Законодательством РК.

*Запрещается несанкционированное ксерокопирование документа*

3) Передача документации при увольнении или переводе на другую работу работников осуществляется в соответствии с должностными инструкциями.
4) Для предотвращения непреднамеренного использования недействующей (отмененной) версии документа, работник Канцелярии изымает из оборота все копии отмененного документа.
5) Копии изъятых документов уничтожаются Канцелярией. Уничтожение производится путем полной утилизации документа, без возможности повторного применения бумаги с целью защиты конфиденциальности сведений и безопасности.
6) Недействительная медицинская документация уничтожается медицинскими работниками, имеющими к ней доступ для выполнения должностных обязанностей согласно Должностной инструкции работника также путем полной утилизации документа, без возможности повторного применения бумаги с целью защиты конфиденциальности сведений и безопасности.

**Использование аббревиатур и сокращений**

При ведении медицинской документации врач, медсестра и иные медработники должны:
1) Писать разборчиво.
2) Если медицинская сестра затрудняется прочитать запись врача, запрещено делать назначения/манипуляции до полного уточнения записи. Запись уточняется у лечащего врача, если нет лечащего – у заведующего, если нет заведующего – у дежурного врача.

**Применение информационных технологий (ИТ)**

1) Участники и пользователи ИТ должны участвовать в выборе, внедрении, и оценке ИТ.
2) Любая внедряемая ИТ должна быть протестирована на практике (пилотный проект) перед внедрением.
3) Любая внедренная ИТ должна быть оценена после внедрения на предмет удобства и обучения пользователей, эффективности и безопасности пациента.
4) Все пользователи ИТ должны обязаны пройти регистрацию и необходимые процедуры.

**9. Защита медицинской документации**

*1)* Информация в медицинской карте является *конфиденциальной.*
2) **Доступ сотрудников** к просмотру и право записи в медицинской карте имеют врачи и средний медперсонал, вовлеченный в лечение и уход за пациентом. Доступ к просмотру записей в медицинской карте также имеют:

– лица, проводящие аудит;
– административно-управленческий персонал с целью проверки счетов на оплату и предоставления сведения о виде и объеме оказанных услуги для плательщиков за медицинские услуги с целью оплаты за услуги;

*Запрещается несанкционированное ксерокопирование документа*

– лица, проводящие научное исследование и публикующие информацию о пациенте без де-идентификации пациента (без сокрытия ФИО, даты рождения) при наличии письменного согласия пациента на участие в научном исследовании;
– лица, проводящие научное исследование или готовящие материалы для участия в медицинской конференции и публикующие информацию о пациенте с де-идентификацией пациента (скрывая ФИО, дату рождения) без письменного согласия пациента на участие в научном исследовании;
– лица, вовлеченные в образовательный процесс: преподаватели, резиденты, курсанты;
– определенный персонал ИТ-службы с разрешения директора и его заместителей.
3) **Доступ пациента** (или его/ее члена семьи, законного представителя) разрешен только к своей медицинской карте.
– Если пациент *еще не выписан*, то на устный запрос посмотреть запись в медицинской карте медперсоналу достаточно показать карту. Для выдачи бумажной копии записи (кроме выписки) необходим письменный запрос от имени пациента на имя лечащего врача (в свободной форме на белом листе с подписью и датой).
– Если пациент *выписан*, любые запросы на копию записей в медицинской карте подаются письменно от имени пациента на имя руководителя центра (заведующего отделения) в свободной форме на белом листе с подписью и датой).
4) Распространение информации из медицинской карты для лиц, не указанных в п. 9.2, разрешено с устного разрешения пациента, если для публикации – то с письменного разрешения пациента.
5) Запрещено выносить медицинскую карту за пределы организации сотрудником или консультантом, имеющим доступ к ней, а также передавать по интернет-ресурсу.
6) После работы (записи, чтения) с медицинской картой, сотрудник должен ее закрыть и хранить в отведенном месте.
7) Бумага, которая содержат информацию о пациенте, *не должна использоваться повторно* (печать на обратной стороне).

**1. Указание условии пересмотра СОП: Пересмотр СОП проводиться 1 раз в 3 года или при появлении новых требовании.**

**2. Нормативные ссылки**:

- Приказ и.о. Министра здравоохранения Республики Казахстан от 30 октября 2020 года «Об утверждении форм учетной документации в области здравоохранения, а также инструкций по их заполнению» № КР ДСМ-175/2020;
-Приказ и.о. Министра здравоохранения Республики Казахстан от 5 ноября 2021 года «Об утверждении стандартов аккредитации медицинских организаций»№ КР ДСМ – 111;
- Закон Республики Казахстан от 7 января 2003 года № 370-II

*Запрещается несанкционированное ксерокопирование документа*

«Об электронном документе и электронной цифровой подписи» (с изменениями и дополнениями по состоянию на 16.05.2018 г.);

- Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 «О Концепции информационной безопасности Республики Казахстан до 2016 года»;

- Постановление Правительства Республики Казахстан от 23 мая 2016 года № 298 «Об утверждении Правил проведения аттестации информационной системы, информационно-коммуникационной платформы «электронного правительства», интернет-ресурса государственного органа на соответствие требованиям информационной безопасности» (с изменениями от 09.04.2018 г.);
- Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты. Свод правил по управлению защитой информации»;
- СТ РК ISO/IEC 27001-2015 Информационная технология Методы и средства обеспечения безопасности Системы менеджмента информационной безопасностью. Требования;

**Лист регистрации изменений**

| № | № раздела, пункта стандарта, в которое внесено изменение | Дата внесения изменения | ФИО лица, внесшего изменения |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

*Запрещается несанкционированное ксерокопирование документа*

## Лист ознакомления

| № | Фамилия И.О. | Должность | Дата | Подпись |
|---|---|---|---|---|
| | Сужинин А.А. | программист | 04.01.2024 | Сух. |
| | Соков А.В | программист | 04.01.2024 | |
| | | | | |
| | | | | |
| | | |