«УТВЕРЖДАЮ»
Главный врач
_____ С.В. Попов
«23» 03 2021г.

ПОЛОЖЕНИЕ
о порядке работы с конфиденциальной информацией в СПб ГБУЗ Клиническая больница Святителя Луки

1. Общие положения

1.1. Настоящее Положение о порядке работы с конфиденциальной информацией (далее по тексту – Положение) в СПб ГБУЗ Клиническая больница Святителя Луки (далее по тексту – Учреждение) устанавливает общие нормы о сведениях, относящихся к категории конфиденциальной информации (в том числе коммерческой тайны, служебной тайны, врачебной тайны), порядок их охраны от недобросовестного использования, определяет единый порядок работы со сведениями, содержащими конфиденциальную информацию работниками Учреждения, порядок допуска к ним и меры ответственности, применяемые за нарушение требований, установленным данным Положением.

1.2. Настоящее Положение разработано с учётом принципов, правил и требований, установленных основными правовыми нормативными актами, регламентирующими требования к процессам обработки персональных данных, соблюдения конфиденциальности, в том числе в медицинских организациях:

- Конституция Российской Федерации;

- Гражданский кодекс Российской Федерации;

- Трудовой кодекс Российской Федерации;

- Кодекс Российской Федерации об административных правонарушениях;

-Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» № 188 от 06.03.1997 г.;

- Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

-Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

- Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

- Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

- Федеральный закон от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств»;

- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»);

- Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

- Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 23.03.2017) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена ФСТЭК 15.02.2008);

- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения;

- ГОСТ 34.603-92 Виды испытаний автоматизированных систем.;

- Модель угроз типовой медицинской информационной системы типового лечебно-профилактического учреждения (Минздравсоцразвития России, ноябрь 2009; согласована с ФСТЭК, письмо от 27.11.2009 № 240/2/4009 за подписью заместителя директора ФСТЭК А.Гапонова);

- Методические рекомендации по организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости (Минздравсоцразвития России, утверждены 23.12.2009 директором Департамента информатизации Минздравсоцразвития России О.В.Симаковым, согласованы 22.12.2009 начальником 2-го управления ФСТЭК России А.В.Куц);

- Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений и организаций здравоохранения, социальной сферы, труда и занятости (Минздравсоцразвития России, утверждены 23.12.2009 директором Департамента информатизации Минздравсоцразвития России О.В.Симаковым, согласованы 22.12.2009 начальником 2-го управления ФСТЭК России А.В.Куц).

- Иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти. и иными нормативными актами, определяющими отношения в сфере работы с конфиденциальной информацией.

1.3. Отношение информации к конфиденциальной осуществляется в порядке, установленном законодательством Российской Федерации. Положение распространяется на сведения, составляющие конфиденциальную информацию Учреждения независимо от вида носителя, на котором они фиксированы (бумажные носители – документы, издания, книги, брошюры и пр.;

магнитные – магнитные диски, цифровые запоминающие устройства, аудио- и видеопленки и пр.; оптические – лазерные диски и пр. и другие носители информации);

1.4. Действие настоящего Положения распространяется на всех работников Учреждения, которые дали обязательство о неразглашении конфиденциальной информации, также на лиц, работающих по гражданско-правовым договорам, заключенным с Учреждением, взявших на себя обязательства по неразглашению конфиденциальной информации, в порядке и на условиях, предусмотренным настоящим Положением.

2. Понятия и термины, используемые в настоящем Положении

2.1. Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с настоящим Положением и включает в себя: коммерческую тайну, врачебную тайну, служебные сведения, персональные данные сотрудников и пациентов, а также любую другую информацию ограниченного использования и доступа.

2.2. Коммерческая тайна – конфиденциальная информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ и услуг или получить иную коммерческую выгоду.

2.3. Информация, составляющая коммерческую тайну – научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую тайну в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

2.4. Врачебная тайна – информация о факте обращения за медицинской помощью, состоянии здоровья пациента, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении в осуществляющих, подразделениях Учреждения, включая все структурные и территориальные подразделения и участки.

2.5. Допуск к сведениям, составляющих конфиденциальную информацию – процедура оформления права доступа работника Учреждения к ознакомлению и работе со сведениями, являющимися конфиденциальными.

2.6. Разглашение сведений, составляющих конфиденциальную информацию – передача в устной, письменной или иной форме, раскрытие и подобные действия, совершенные работником Учреждения умышленно или по неосторожности, включая халатное отношение к своим должностным обязанностям, повлекшее ознакомление со сведениями, относящимися к конфиденциальной информации Учреждения, любых лиц, не имеющих права доступа на законном основании к указанным сведениям.

3. Сведения, относимые к конфиденциальной информации Учреждения

3.1. Сведения, относящиеся к конфиденциальной информации:

3.1.1. Сведения о фактах, обстоятельствах и событиях частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

3.1.2. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, тайна переписки, телефонных разговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

3.1.3. Сведения, содержащиеся в служебной переписке, телефонных переговорах, почтовых отправлениях, телеграфных или иных сообщениях, передаваемых по сетям электронной или почтовой связи, которые стали известны работнику Учреждения в связи с исполнением им возложенных на него трудовых обязанностей.

3.1.4. Разновидностью конфиденциальной информации являются сведения, относящиеся к коммерческой тайне Учреждения, имеющие признаки перечисленные в п. 2.2 настоящего Положения:

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами;
- сведения о созданных или создаваемых объектах интеллектуальной собственности Учреждения, на получение которых не имеется разрешение Учреждения;
- сведения, содержащиеся в учредительных, организационно-распорядительных, финансово-экономических документах (в письменной форме или на электронных носителях), а также полученные в устной форме на совещаниях, заседаниях и переговорах.

3.1.5. К сведениям, составляющим коммерческую тайну Учреждения, не относятся сведения, которые указаны в ст. 5 Федерального закона № 98-ФЗ от 01.01.2001 года «О коммерческой тайне», Постановлении Правительства РСФСР от 29.071.2004 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

4. Порядок отнесения сведений к категории конфиденциальной информации Учреждения

4.1. Отнесение сведений к категории конфиденциальной информации осуществляется путем введения ограничений на разглашение и доступ к ее носителю в следующем порядке:

4.1.1. В случае наличия действительной, потенциальной или иной ценности какой-либо информации, руководитель структурного подразделения письменно уведомляет об этом главного врача Учреждения. Решение о защите прав Учреждения на данный объект путем отнесения сведений о нем к категории конфиденциальной информации принимает главный врач Учреждения.

4.1.2. При принятии решения о целесообразности защиты прав Учреждения на данный конкретный объект путем отнесения ключевых сведений о нем к категории конфиденциальной информации Учреждения, главным врачом издается приказ, содержащий:

- название объекта,
- краткую характеристику объекта, содержащую его идентификацию,
- перечень охраняемых сведений,
- срок охраны указанных сведений,
- указание ответственного лица за проведение мероприятий, направленных на охрану сведений об объекте.

4.1.3. Приказ, изданный главным врачом, доводится до руководителя работ и руководителя соответствующего подразделения Учреждения.

4.1.4. В перечень охраняемых сведений об объекте включается лишь то количество сведений, несанкционированное Учреждением разглашение или передача которых другим организациям и лицам могут лишить объект его ценности для Учреждения. Содержание охраняемых сведений в тексте распоряжения не разглашается.

4.1.5. Учет сведений, относящихся к категории врачебной тайны, ведут все структурные подразделения Учреждения, осуществляющие медицинскую деятельность.

4.1.6. Сводный учет сведений, относящийся к коммерческой тайне, осуществляет руководитель подразделения, в ведении которого находится подразделение по осуществлению коммерческой деятельности Учреждения.

4.1.7. Сводный учет данных, относящихся к служебным сведениям (ДСП – для служебного пользования), осуществляет канцелярия, ведущая документооборот Учреждения.

4.1.8. Сводный учет данных о сотрудниках, имеющих доступ к конфиденциальной информации осуществляет отдел управления персоналом Учреждения, который фиксирует в соответствующих документах фамилию, имя, отчество работника, номер и дату издания приказа о допуске его к конфиденциальной информации, перечень документов, к которым он допущен.

5. Порядок оформления и прекращения допуска к конфиденциальной информации

5.1. Принятие на себя обязательства о неразглашении конфиденциальной информации осуществляется работником на добровольной основе.

5.2. На основании распоряжения или приказа об отнесении сведений к категории конфиденциальной информации Учреждения, руководитель структурного подразделения составляет список сотрудников, ознакомленных с указанными сведениями или с частью этих сведений в связи с выполнением служебных обязанностей. Сотрудник, который в силу своих обязанностей имеет доступ к сведениям, составляющим конфиденциальную информацию, а также сотрудник, которому будет открыть доступ к сведениям, относящимся к конфиденциальным данным для исполнения определенного задания, обязан при приеме на работу либо по первому требованию ознакомиться с настоящим Положением и дать обязательство о неразглашении сведений. Составляющих конфиденциальную информацию. Руководитель структурного подразделения организует ознакомление перечисленных в списке сотрудников с распоряжением и получение от сотрудников (в том числе и от руководителя работ) расписок о том, что они ознакомлены с распоряжением. Подлинник распоряжения с расписками сотрудников передается в отдел кадров. Копия распоряжения хранится у руководителя структурного подразделения.

5.3. Доступ к сведениям, составляющим конфиденциальную информацию, осуществляется только после дачи сотрудником соответствующего обязательства.

5.4. Доступ сотрудника к сведениям, относящихся к конфиденциальной информации, может быть прекращен в следующих случаях:

- прекращение трудового договора (независимо от причин прекращения);
- однократное нарушение им взятых на себя обязательств, связанных с неразглашением и охраной конфиденциальной информации;
- по инициативе руководства. Прекращение доступа оформляется в виде приказа, который доводится до сведения сотрудника под роспись.

6. Меры по охране конфиденциальной информации Учреждения

6.1. Необходимым условием принятия решения о возмещении ущерба со стороны организаций и лиц, нарушивших его права, незаконно присвоивших, использовавших или разгласивших сведения, относящиеся к конфиденциальной информации, является осуществление Учреждением действий по обеспечению достаточной защиты указанных сведений от их несанкционированного использования и (или) распространения.

6.2. Руководитель структурного подразделения, сотрудники Учреждения, имеющие доступ к сведениям, составляющим конфиденциальную информацию Учреждения, обеспечивают защиту указанных сведений путем:

- ограничения доступа к указанным сведениям для посторонних лиц и для сотрудников Учреждения, непосредственно не связанных с этими сведениями (в том числе путем

организации надлежащего хранения физических носителей информации, таких как документация, электронные носители);

- соблюдение установленных в Учреждении правил работы с электронными устройствами и каналами, хранения, обработки и передачи информации (в том числе путем использования криптографии и средств защиты информации от несанкционированного доступа);
- неразглашения сведений, составляющих конфиденциальную информацию Учреждения, документации, служебных и неслужебных разговоров и т. п.;
- передачи другим лицам и организациям сведений, содержащих конфиденциальную информацию Учреждения только в рамках оферт и договоров, заключенных этими организациями и лицами с Учреждением, с отражением в тексте договора, оферты обязательств получающей стороны соблюдать конфиденциальность полученной информации. Объем передаваемых сведений и условия передачи определяются руководителем работы и руководителем структурного подразделения Учреждения.

6.3. Документы (в том числе на электронных носителях), содержащие конфиденциальную информацию Учреждения хранятся у руководителей работ или у руководителей структурных подразделений. Без разрешения руководителя структурного подразделения запрещается выносить документы из кабинетов. Запрещается оставлять документы без присмотра на рабочих местах, в общедоступных помещениях. При хранении данных, содержащих конфиденциальную информацию Учреждения, на персональных компьютерах (ПК), обеспечивается защита от несанкционированного доступа к этим данным и их несанкционированной передачи. Также запрещается допуск посторонних лиц к ПК с конфиденциальной информацией. Перечень подлежащих выполнению конкретных мероприятий определяется особенностями охраняемых сведений. Организацию работ по информационной защите конфиденциальных данных осуществляет отдел, в ведении которого находятся сотрудники выполняющие мероприятия по системно-технологическому обеспечению и информационным технологиям. Контроль за обеспечением информационной защищенности осуществляет инженер по обеспечению информационной безопасности Учреждения.

6.4. Содержание конкретных мероприятий по охране сведений, являющихся конфиденциальной информацией Учреждения, разрабатывается руководителем работ совместно с руководителем структурного подразделения, в котором эти сведения сосредоточены. Содержание этих мероприятий согласовывается с инженером по обеспечению информационной безопасности Учреждения.

6.5. Для обозначения документов, содержащих конфиденциальную информацию, в верхнем правом углу проставляется реквизит «КИ» или «Конфиденциальная информация». Документы с таким реквизитом хранятся, обрабатываются и пересылаются как аналогичные документы с грифом «ДСП» или «Для служебного пользования».

6.6. Копирование информации, содержащей конфиденциальную информацию разрешается только с письменного разрешения руководителя структурного подразделения. На первом экземпляре документа (носителе), с которого снимается копия делается отметка о лице, копировавшем информацию, дате и количестве копий. Руководитель структурного подразделения Учреждения организует контроль выполнения мероприятий по защите конфиденциальной информации Учреждения, привлекая по необходимости специалиста по защите информации.

6.7. В целях защиты конфиденциальной информации Учреждения сотрудники Учреждения, допущенные к ней, обязаны:

6.7.1. Выполнять установленный в Учреждении режим конфиденциальной информации;

6.7.2. Не разглашать информацию, составляющую конфиденциальную информацию, обладателем которой является Учреждение и его контрагенты, и без их согласия не использовать эту информацию в личных целях;

6.7.3. Не разглашать информацию, составляющую конфиденциальную информацию, обладателем которой является Учреждение и его контрагенты, в течении 3-х лет после прекращения трудового договора;

6.7.4. Возместить причиненный Учреждению ущерб, если сотрудник виновен в разглашении информации, составляющей конфиденциальную информацию, ставшей ему известной в связи с исполнением им своих трудовых обязанностей;

6.7.5. Сообщать непосредственному начальнику, руководителю структурного подразделения Учреждения о всех ставших ему известных фактах утечки сведений, составляющих конфиденциальную информацию Учреждения, а также об утрате документов с грифом «КИ» или «Конфиденциальная информация»;

6.7.6. Передать Учреждению при прекращении или расторжении трудового договора, имеющиеся в пользовании материальные носители информации, содержащие сведения, составляющие конфиденциальную информацию.

7. Ответственность за нарушение конфиденциальности информации

7.1. В случае разглашения конфиденциальной информации, ставшей известной работнику в связи с исполнением им своих трудовых обязанностей, в том числе разглашением им персональных данных другого работника, трудовой договор с работником может быть расторгнут по инициативе работодателя в соответствии с трудовым законодательством.

7.2. Собирание сведений, составляющих конфиденциальную информацию, путем похищения документов, подкупа или угроз, а равно иным незаконным способом влечет уголовную ответственность в соответствии с законом.

7.3. Разглашение конфиденциальной информации (за исключением случаев, когда разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей влечет дисциплинарную, гражданско-правовую и административную ответственность и (или) материальную ответственность.

7.4. Возмещение ущерба, причиненного Учреждению в связи с нарушением прав учреждения на его конфиденциальную информацию, производится в установленном законом порядке, организациями и лицами (в том числе работниками Учреждения), нарушившими действующее законодательство и указанные права.

7.5. Ответственность в соответствии с действующим законодательством, несут также работники и должностные лица Учреждения, не выполнившие или не обеспечившие выполнение требований настоящего Положения и тем самым способствовавшие нарушению конфиденциальности информации, а также не принимавшие необходимых и достаточных мер по пресечению ставших им известных фактов нарушения прав Учреждения.

7.6. На основании информации о фактах нарушения прав Учреждения на его конфиденциальную информацию руководство Учреждения, при не достижении договоренности об удовлетворении претензий, принимает меры по восстановлению и защите нарушенных прав и возмещению причиненного ущерба.

8. Заключительные положения

8.1. Настоящее Положение вступает в силу с момента его утверждения главным врачом учреждения.