

**Организация обработки
персональных данных в
медицинских учреждениях:
правовые основы и новые
требования**

проф., д.т.н. Столбов А.П.

Москва, РАМН, 28 февраля 2008 г.

**Конституция Российской Федерации (12.12.1993 г., ред. ... от 21.07.07 г. № 5-ФКЗ),
ст. 23, 24 (неприкосновенность частной жизни, личная и семейная тайна),
ст. 41, 42 (недопустимость сокрытия информации ... угроза жизни и здоровью)**

Закон "Об информации, информационных технологиях и защите информации", № 149-ФЗ от 27.07.2006 г.

Закон "О персональных данных", № 152-ФЗ от 27.07.2006 г. !!!

**Основы законодательства Российской Федерации об охране здоровья граждан, № 5487-1 от 22.07.1993 г. (ред. ... от 18.10.07 г. № 230-ФЗ)
ст. 19, 30, 31, 32, 33, 34, 61 ***

Закон "О медицинском страховании граждан в Российской Федерации, № 1499-1 от 28.07.1991 г. * (ред. ... от 29.12.06 г. № 258-ФЗ) [ст. 12 ведение баз данных]

Об утверждении перечня сведений конфиденциального характера, Указ Президента РФ № 188 от 06.03.1997 г. (в ред. Указа Президента РФ от 23.09.05 г. № 1111)

Закон "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования", № 27-ФЗ от 01.01.1996 г. (ред. ... от 19.07.07 г. № 140-ФЗ) [как модельный закон]

Закон "Об электронной цифровой подписи", № 1-ФЗ от 10.01.2002 г. (ред. от 08.11.07 г. № 258-ФЗ)

Постановление Правительства РФ от 17.11.07 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"

ПЕРСОНАЛЬНЫЕ ДАННЫЕ -- сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность

КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ -- документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации

ОБЛАДАТЕЛЬ информации -- лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [кто? врач и\или пациент ?] *

ПРЕДОСТАВЛЕНИЕ информации -- действия, направленные на получение информации определенным кругом лиц

РАСПРОСТРАНЕНИЕ информации -- действия ... получение информации НЕопределенным кругом лиц

ВРАЧЕБНАЯ ТАЙНА -- информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении (ст. 61 "Основ...об охране здоровья...")

Закон "О персональных данных", № 152-ФЗ от 27.07.2006 г.

- документированное (!!!) согласие пациента на обработку и передачу его персональных данных и обязанность оператора предоставить доказательства этого согласия (см. письмо ФФОМС от 17.10.2000 г. № 4827/91-и)
- обязанность оператора предоставить субъекту информацию об обработке его персональных данных, полученных ИЗВНЕ на законных основаниях
- уведомление (!!!) об обработке персональных данных (реестр операторов)

Приказ Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия (Россвязьохранкультура) от 11.01.08 г. № 3 "Об утверждении формы уведомления об обработке (о намерении осуществлять обработку) персональных данных" (www.rsoc.ru)

Форма уведомления + Рекомендации по его заполнению

- реквизиты оператора обработки персональных данных
- цель обработки (**медицинский учет**)
- категории перс. данных (паспортные данные, состояние здоровья)
- категории субъектов перс.данных (гражд.РФ, иностр.гражд., лица без гражд.)
- правовое обоснование (законы, решения правительства, регламенты ...) !!!
- способы обработки (сбор, накопление, хранение, изменение, удаление ...)
- меры по защите информации (разграничение доступа, сертифицированные средства защиты, отключение от Интернет ...)

ПОЛИЦЕВОЙ учет медицинской помощи -- осуществляемое по установленным правилам документирование процесса и результатов обследования и лечения пациента в медицинском учреждении. При передаче данные полицевого учета могут быть представлены в виде записей (документов):

- персонифицированных = { ID, Пд, Рд, Сд, Ад, Мд }
- деперсонифицированных = { ID, Рд, Сд, Ад, Мд } **!!!**
- обезличенных = { Рд, Сд, Ад, Мд }

где ID -- СНИЛС, номер полиса ОМС, номер паспорта etc.

Пд -- Ф.И.О., адрес места жительства, место работы **!!!**

Рд -- пол и дата рождения пациента

Сд -- социально-демографические данные

Ад -- административные данные, Мд -- медицинские данные

Записи вида { ID, Пд,... }, { Пд,... } конфиденциальны (служебная тайна)

Деперсонифицированный регистр в сети Интернет ("номерник")

{ ID*, дата рожд., пол?, 3 буквы ФИО?, коды ТМЖ, льгот, ... , Даты* ... }

ЗАЩИТА ИНФОРМАЦИИ -- комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным.

Концепция обеспечения информационной безопасности в системе ОМС на период до 2010 года (утв. в 2005 г.) *

Приказ ФФОМС от 25.03.1998 г. № 30 "О соблюдении конфиденциальности сведений, составляющих врачебную тайну"

- Издание организационно-распорядительных документов о допуске персонала и регламентах обработки конфиденциальной информации
- Аттестация, регистрация и аудит ИС для допуска к обработке конфиденциальной информации (см. www.infotecs.ru *)

ГОСТ Р ИСО/МЭК 15408-1,2,3-2002 Критерии оценки безопасности информационных технологий. Функциональные требования безопасности

ГОСТ Р ИСО/МЭК ТО 13335-5-2006, 13335-1,3,4-2007 Информационная технология. Методы и средства обеспечения безопасности.

ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

СПАСИБО !

ВОПРОСЫ?

Столбов Андрей Павлович

stolbov@mcramn.ru

ap100lbov@mail.ru

www.mcramn.ru