

- стремление к «внешней» взрослости, подражание значимым для подростка людям (положительные и отрицательные привычки, особенности лексики, манеры поведения взрослых, развлечения, досуг);
- равнение на настоящего мужчину, демонстрация мужества, воли, силы, смелости, настойчивости вплоть до крайности: совершение отчаянных, безрассудных, асоциальных поступков;
- жажда приобщения к делам и отношениям взрослых, сотрудничество с взрослыми в разных сферах деятельности, желание обрести профессиональные навыки, нести социальную ответственность, реализация потребностей в общественном признании, быть независимым в материальных средствах;
- повышение мотивации в сфере познавательной деятельности, стремление к обогащению знаний в области науки, искусства, самообразование (Сосновский Б.А. М., 2009).

Исследователями обозначены три ступени формирования самосознания: первая ступень связана с индивидуально-психологическими особенностями (общая конституция, психосоматические процессы, чувствительность, биохимические, биофизические, биоэнергетические показатели, внешний облик); вторая - определяется как личностная и характеризуется особенностями подростковой деятельности, мотивационной сферы, направленности личности подростка и жизненного самоопределения; третья ступень – это поведенческие нормы подростков, их адаптивность в средовом окружении, особенности формирования мировоззрения, нравственных идеалов, приобщение к национальным культурным традициям, обычаям, воздействие социальных институтов: семьи, школы, детских формальных объединений, СМИ, религии.

Все стадии формирования самосознания достойны широкого обсуждения, между тем, неоспорим тот факт, что третья ступень наиболее подвержена влиянию семьи, так как именно в семейной микросреде при адекватном родительском отношении повышается самооценка подростка, формируется самоуважение к себе как равноправному члену общества.

Литература/References:

1. Фельдштейн Д.И. Особенности стадий развития личности на примере подросткового возраста // Психология развития личности в онтогенезе. – М., 1989.
2. Практическая психология образования: Учебник для студентов высших и средних специальных учебных заведений. // Под ред. И.В.Дубровиной. – М.: Ц «Сфера», 1998.
3. Психология: Учебник для Педагогических вузов/Под ред. Б.А.Сосновского – М.: Высшее образование, 2009.
4. Кон И.С. Психология ранней юности – М.: Просвещение, 1989.
5. Божович Л.И., Этапы формирования личности в онтогенезе. // «Вопросы психологии», 1979, №2,4.
6. Хайдарова Д.К., Ходжаева Д.Т. Наука и общество от теории к практике. Монография. Ставрополь “Логос” 2016
7. Хайдарова Д.К., Ходжаева Д.Т. Наука о человеке- от Авиценны до современности. Монография – Бухара- 2018.

УДК: 61.68:578.834.1-004.056.5

ЗАЩИТЫ ДАННЫХ В ПЕРИОД ПАНДЕМИИ COVID-19

Атамуратова Феруза Садуллаевна¹, Рахманова Сарвиноз²

Ташкентская медицинская академия, Узбекистан, Ташкент

1. Доцент кафедры Социальных наук
fatamur@mail.ru
2. Рахманова Сарвиноз
Студентка 6 курса лечебного факультета
srahmanova014@gmail.com

Аннотация. Ни для кого не секрет, что с развитием информационных технологий, обострились многие этические проблемы биомедицины. Особенно это касается вопроса врачебной тайны, защиты данных пациента.

Цифровая медицина, особенно в чрезвычайных ситуациях, ставит противоположное требование - разглашать все данные о течении заболевания в целях уменьшения дальнейшего его распространения. В период пандемии COVID-19, каждый день в СМИ мы читаем или смотрим видео со всего мира о заболевших людей и о том, как протекают их болезни. Защита конфиденциальности персональных данных, информирование и программная поддержка пользователя, обоснованность применения мобильных медицинских приложений, относятся к числу важных с этической точки зрения телемедицины и этических проблем. Многие люди конечно же не хотят, чтобы его личные данные становились центром обсуждения. С другой стороны, сбор, хранение, распространение и дальнейшая обработка некоторых данных могут способствовать ограничению распространения вируса. Найти баланс в этой нелегкой ситуации очень сложно. Поэтому, считаем, необходимо пересмотреть многие этические проблемы в чрезвычайных условиях и разработать новые аргументы в пользу прав человека.

Ключевые слова. COVID-19, пандемия, утечка данных, этика, врачебная тайна

Ни для кого не секрет, что с развитием информационных технологий, обострились многие этические проблемы биомедицины. Особенно это касается вопроса врачебной тайны, защиты данных пациента. Еще великий Гиппократ в своей «Клятве» писал, «... Что бы при лечении — а также и без лечения — я ни увидел или ни услышал касательно жизни людской из того, что не следует когда-либо разглашать, я умолчу о том, считая подобные вещи тайной...» [1].

Понятие «врачебной тайны» сегодня широко используется в юриспруденции и медицине. Врачебная тайна - медицинское, правовое, социально-этическое понятие, представляющее собой запрет медицинскому работнику сообщать третьим лицам информацию о состоянии здоровья пациента, диагнозе, результатах обследования, самом факте обращения за медицинской помощью и сведениях о личной жизни, полученных при обследовании и лечении [2]. Врачебная тайна защищает права пациента и охраняется законом. В частности, в Законе Республики Узбекистан «Об охране здоровья граждан» в статье 45 регламентируется, что «Информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну» [3]. Кроме выше перечисленного, согласно законодательству Республики Узбекистан, во врачебную тайну следует отнести персональные данные пациента начиная от ФИО, информации о дате и месте рождения, антропометрических показателей (рост, вес), фотографий, места жительства, контактных номеров, и до сведений о болезнях, результатов анализов и методов лечения. Разглашать врачебную тайну запрещено даже после смерти пациента. При этом медицинские учреждения обязаны хранить данные о здоровье каждого обратившегося человека в виде медицинской карты. Человек, обращаясь в медицинское учреждение и разглашая всю информацию о себе должен быть уверен, что его данные будут сохранены конфиденциально. Следует обратить внимание, что сохранение врачебной тайны

является моральной обязанностью врача. Ее незаконное разглашение - признак профессиональной непригодности или неопытности данного врача.

В век информационных технологий, развития «цифрового здравоохранения» и «цифровой медицины» вопрос «врачебной тайны», особенно, касающийся защиты данных пациента стал большой проблемой. Сегодня информационные технологии в деятельности медицинских организаций охватывают практически все стороны их деятельности, включая управление ресурсами, лечебным процессом и оказание медицинской помощи.

Информационные технологии в медицине дают возможность проводить качественное наблюдение за состоянием пациентов. Ведение электронных медицинских карт позволяет сократить время сотрудников клиник, потраченное на оформление различных бланков. Вся информация о пациенте представлена в одном документе, доступном медицинскому персоналу учреждения. Все данные об обследованиях и результаты процедур также вводятся непосредственно в электронную медицинскую карту. Это дает возможность другим специалистам оценить качество назначенного лечения, обнаружить неточности диагностики.

Применение ИТ в медицине позволяет врачам проводить онлайн-консультации в любое удобное время. При этом повышается доступность медицинских услуг. Люди могут получить квалифицированную помощь от опытных врачей удаленно. Это особенно необходимо людям: проживающим в географически удаленных районах; с ограниченными физическими возможностями; попавшим в чрезвычайную ситуацию; которые находятся в замкнутом пространстве [4].

В рамках Государственной программы, 2020 год - Год развития науки, просвещения и цифровой экономики, разработаны, а также реализованы ряд задач и проектов в соответствии с поручениями Президента Республики Узбекистан. В соответствии с постановлением Президента «О мерах по широкому внедрению цифровой экономики и электронного правительства» как основополагающим документом по дальнейшей цифровизации страны на ближайшие годы в период 2020-2022 годов намечено осуществить 12 проектов в сфере здравоохранения. К примеру, внедрение информационной системы «Электронная медицинская карта пациента» позволит сформировать единую базу медицинских данных о гражданах Республики Узбекистан, проводить мониторинг здоровья населения; внедрение информационной системы «Электронный рецепт» позволит организовать систему эффективного и безопасного лечения пациентов медикаментозными препаратами и сформировать электронный реестр врачей, совершенствовать систему контроля и мониторинга лекарственных средств; с целью качества оказываемых медицинских услуг путем создания современной компьютеризированной системы в лечебных медицинских учреждениях планируется осуществление проектов по внедрению информационных систем «Электронная поликлиника» и «Электронная больница»; хорошей научно-практической базой для исследовательских работ в сфере здравоохранения может стать проект «Лаборатория», в чьи задачи входит формирование электронного реестра анализа, показателей и других данных. Сфере здравоохранения в вопросах цифровизации сферы государственных услуг отведено центральное место. Как отмечается в государственной программе, все вышеназванные проекты носят актуальный и важный характер, и их реализация позволит повысить качество жизни наших граждан, усовершенствовать систему здравоохранения в Республике.

Но этическая сторона данного вопроса, как было сказано, является весьма проблемной. К примеру, в Китае права на сбор, обмен, использование, управление данными законодательно регулируются, но передаются как государственным, так и частным компаниям. Большие объемы данных становятся доступны широкому кругу исследователей, что, безусловно, способствует развитию современных технологий, но в ущерб приватности частных лиц. Кроме того, персональные данные, в том числе о состоянии здоровья или различных склонностях, сообщают о себе сами люди, делясь своими переживаниями в социальных сетях, собираются данные о посещении различных

медицинских учреждений; покупки или поиск соответствующих товаров в интернет-магазинах, запросы о лекарственных препаратах или лечении недугов отслеживаются различными поисковыми системами. По международному законодательству каждый пользователь, регистрирующийся на сайте, имеет право изменить свои настройки приватности или требовать немедленного удаления своих персональных данных. Закон о защите персональных данных запрещает использование персональных данных для каких-либо целей, кроме тех, на которые владелец этих данных конкретно согласился. Без разрешения со стороны пользователя строить профайлы, рассылать рекламу, анализировать покупки, передавать или продавать данные институтам, научным организациям нельзя. Кроме того, любой человек может запросить у компании, какие данные она на него держит, и если захочет, то потребовать, чтобы эти данные были уничтожены. За нарушение правил – штраф в размере до 4% годового оборота компании [5].

Результаты анонимного опроса, специалистов Центра подготовки руководителей и команд цифровой трансформации (РКЦТ), проведенного 05.04.2021 года, причастных к разработке или эксплуатации государственных цифровых сервисов доказывают, что, основная масса людей не согласны оглашать свои персональные данные для общественности. К примеру, главной этической проблемой при создании и использовании цифровых технологий респонденты считают неправильное обращение с персональными данными (ПДн). 83% опрошенных считают наиболее критичной утечку ПДн, также вызывают опасения риск передачи данных третьим лицам (72%) и сбои, и поломки инфраструктуры (57%): цифровой мир респонденты воспринимают как во многом непрочный и ненадежный. Отдельно предлагалось оценить, насколько критичен риск недостаточной защиты ПДн — и 98% опрошенных говорят о той или иной степени критичности этой проблемы [6, 20].

«Утечка данных» имела особое место в период пандемии COVID-19. Экспертно-аналитический центр ГК InfoWatch опубликовал исследование, посвященное изучению случаев утечек конфиденциальной информации, относящейся к COVID-19. За первое полугодие 2020 г. зафиксировано 72 случая преднамеренной или случайной утечки в мире. Практически половина всех случаев утечек, связанных с COVID-19 в мире, произошла из медицинских учреждений, на их долю пришлось более 43% всех утечек по теме COVID-19 [7]. Один из наиболее масштабных инцидентов — компрометация данных более 1 млн американских медиков. Кроме того, хакеры получили доступ к личным данным больных коронавирусом Катара — через уязвимость в приложении, которое граждане устанавливали по требованию правительства. В мае в руки гражданских журналистов из некоммерческой организации 100Reporters попали документы, проливающие свет на то, как Китай собирал данные о распространении коронавирусной инфекции среди своего населения. В файлах было представлено около 640 тыс. «обновлений», то есть строк, где отображены выявленные случаи заражения COVID-19 [8].

Журнал HIPAA ((Health Insurance Portability and Accountability Act) Закон о переносимости и подотчетности в сфере медицинского страхования) опубликовал статистику утечек данных в сфере здравоохранения в 2020 году. Приведенные данные ясно показывают, что за последние 10 лет наблюдается тенденция к увеличению количества утечек данных, причем в 2020 году было зарегистрировано больше нарушений данных, чем в любой другой год. с тех пор, как записи впервые начали публиковаться.

За прошедшие годы также произошли заметные изменения в основных причинах нарушений. В отчетах о нарушениях в период с 2009 по 2015 гг. Преобладала потеря / кража медицинских записей и защищенной электронным способом медицинской информации. Более совершенные политики и процедуры, а также использование шифрования помогли уменьшить эти легко предотвратимые нарушения. Наша статистика утечки медицинских данных показывает, что основными причинами утечки медицинских данных в настоящее время являются взломы / ИТ-инциденты, при этом инциденты несанкционированного доступа / раскрытия также являются обычным явлением.

В период с 2009 по 2020 год в Управление по гражданским правам ННС было сообщено о 3705 нарушениях медицинских данных из 500 или более записей. Эти нарушения привели к потере, краже, раскрытию или недопустимому разглашению 268 189 693 медицинских записей. Это составляет более 81,72% населения США. В 2018 году об утечках данных в области здравоохранения 500 или более записей сообщалось примерно по 1 раз в день. В декабре 2020 года этот показатель увеличился вдвое. Среднее количество нарушений в день за 2020 год составило 1,76. [9] По данным Управления по гражданским правам (OCR), в 2016 году было зарегистрировано более 322 случаев нарушения данных в сфере здравоохранения. Это только те дела, в каждом из которых было зарегистрировано более 500 записей. Год завершился открытием более 16 миллионов записей, в основном от поставщиков медицинских услуг. Фактически, отрасль здравоохранения является наиболее уязвимой для нарушений конфиденциальности. Киберпреступники считают медицинские данные ценными, поскольку они содержат информацию, достаточную для кражи личных данных, и хранятся в ней всю жизнь. В отличие от финансовых данных, которые теряют ценность при изменении или замене, медицинские данные являются постоянными, и киберпреступники могут многократно использовать их для различных преступных действий, таких как мошенничество и злоупотребления в области медицинского страхования. Для киберпреступников это более прибыльно, чем простая продажа украденных данных на подпольном рынке. В целом, взлом остается основной причиной утечки данных в сфере здравоохранения, за которой следует несанкционированный доступ.

Киберпреступники также считают, что медицинские организации легко атаковать, потому что многие из них не применяют адекватные меры безопасности и методы. Согласно опросу, в секторе здравоохранения самые низкие показатели шифрования данных: только 31% учреждений сообщили о широком использовании шифрования.

В то время как медицинские организации осведомлены о финансовых последствиях нарушений HIPAA из-за утечки данных, многие организации по-прежнему пытаются управлять конфиденциальностью данных. В июле 2016 года государственный университет в Орегоне согласился урегулировать потенциальные нарушения на сумму 2,7 миллиона долларов за множественные нарушения: два сообщения касались незашифрованных ноутбуков, а другой - украденного незашифрованного флэш-накопителя. [10]

Такое большое количество утечек может быть в первую очередь связано с тем, что к теме коронавируса у общества повышенный интерес, соответственно, активизируются злоумышленники, которые целенаправленно похищают данные. Кроме того, сами люди, которые работают в сферах, связанных с COVID-19, часто распространяют персональную информацию – умышленно или по незнанию. Внештатный режим работы многих организаций во время эпидемии также способствовал тому, что стандарты обработки и хранения персональных данных могли быть нарушены.

Основным каналом утечек информации, связанной с пандемией, стала Сеть. В 64,2% случаев во всем мире персональные данные, относящиеся к пандемии COVID-19, были скомпрометированы в виде списков - отдельные документы, сводки, фрагменты записей. Нарушители фотографировали списки, набирали увиденную или услышанную информацию на своих устройствах, после чего в большинстве случаев распространяли ее через мессенджеры или группы в социальных сетях [11].

Одним из таких случаев является распространение данных о нулевом пациенте COVID-19 в Республике Узбекистан [12]. В сети широко обсуждалась информация не только о ней, но и обо всех ее близких родственниках. Были данные включая фамилии, имена, возраст, место работы, течение заболеваемости и т.д. И таких случаев утечки информации наблюдались во всем мире.

В этих условиях заявление генерального секретаря ООН в период пандемии стала ключевым моментом в этой этической проблеме. В своей [аналитической записке](#) он отметил, что «... Любой сбор, использование и обработка данных учреждениями системы ООН в контексте пандемии COVID-19 должны основываться на правах человека и осуществляться с

должным учетом применимых норм международного права и принципов защиты данных и неприкосновенности частной жизни, включая Принципы ООН, касающиеся защиты личных данных и неприкосновенности частной жизни» [13].

Многие государства приняли соответствующие меры, касающиеся в сфере защиты персональных данных ещё до пандемии. К примеру, Закон Республики Узбекистан «О персональных данных» был принят в июле 2019 года и вступил в силу с 1 октября того же года. Документ дополнен статьёй 27–1 «Особые условия обработки персональных данных граждан Республики Узбекистан». Она гласит: «Собственник и (или) оператор при обработке персональных данных граждан Республики Узбекистан с использованием информационных технологий, в том числе во всемирной информационной сети Интернет, обязан обеспечить их сбор, систематизацию и хранение в базах персональных данных на технических средствах, физически размещенных на территории Республики Узбекистан и зарегистрированных в установленном порядке в Государственном реестре баз персональных данных» [14].

В современном мире специалистами предлагаются новые идеи и концепции, а также разрабатываются различные программы и платформы для защиты базы данных. Одной из таких новшеств является книга «Базы данных. Инжиниринг надежности» авторов Лейна Кэмпбелла и Черити Мейджорса. Может быть, предлагаемые платформы смогут решить данную этическую проблему.

Литература/References:

1. Словарь терминов // <https://tass.ru/obschestvo/7722927> [Slovar terminov // <https://tass.ru/obschestvo/7722927>]
2. Перевод В. И. Руднева. Гиппократ. Избранные книги. М., 1994. С.87-88. ISBN 5-85791-011-0 [Perevod V. I. Rudneva. Hippokrat. Izbrannye knigi. M., 1994; 87-88 (InRuss)]
3. Закон Республики Узбекистан «Об охране здоровья граждан»// <https://www.lex.uz/acts/41329> [Zakon Respubliki Uzbekistan “Ob ohrane zdorovya grajdan”// <https://www.lex.uz/acts/41329> (InRuss)]
4. Информационные технологии в медицине // <https://robo-med.com/articles/informatsionnye-tekhnologii-v-meditsine/> [Informatsionnyie texnologii d meditsine // <https://robo-med.com/articles/informatsionnye-tekhnologii-v-meditsine/> (InRuss)]
5. Цифровая революция в здравоохранении: достижения и вызовы развития // <https://tass.ru/pmef-2017/articles/4278264> [Tsifrovaya revolyutsiya v zdravoohranenii dostijeniya i vyzovy razvitiya <https://tass.ru/pmef-2017/articles/4278264> (InRuss)]
6. Этика и «цифра»: от проблем к решениям/ под ред. Е. Г. Потаповой. - М.: РАНХиГС, 2021. [Etika i “tsifra”: ot problem k resheniyam/ pod red. Ye. G. Potapovoy.- M.: RANXiGS, 2021 (InRuss)]
7. COVID-19 раздал 3,5 млн персональных данных // COVID-19 раздал 3,5 млн персональных данных | ComNews [COVID-19 razdal 3,5 mln personalnyh dannyh // COVID-19 razdal 3,5 mln персональных данных | ComNews (InRuss)]
8. Кто нас знает: треть утечек данных пациентов с COVID-19 прихлась на Россию | Статьи | Известия // <https://iz.ru/1043482/anastasiia-gavriliuk/kto-nas-znaet-tret-utechek-dannykh-patcientov-s-covid-19-prishlas-na-rossiiu> [Kto nas znaet: tret' utechek dannyh pacientov s COVID-19 prishlas' na Rossiyu | Stat'i | Izvestiya // <https://iz.ru/1043482/anastasiia-gavriliuk/kto-nas-znaet-tret-utechek-dannykh-patcientov-s-covid-19-prishlas-na-rossiiu> (InRuss)]
9. <https://iz.ru/1043482/anastasiia-gavriliuk/kto-nas-znaet-tret-utechek-dannykh-patcientov-s-covid-19-prishlas-na-rossiiu> (InRuss)]

10. Healthcare data breach statistics <https://www.hipaajournal.com/healthcare-data-breach-statistics/>
11. 2016 Breaches of healthcare data <https://blog.caspio.com/healthcare-data-breaches/>
12. COVID-19: пандемия спровоцировала утечку 3.5 млн записей персданных в мире // <https://www.infowatch.ru/company/presscenter/news/28596> [COVID-19: pandemiya sprovocirovala utechku 3.5 mln zapisej persdannyh v mire <https://www.infowatch.ru/company/presscenter/news/28596> (InRuss)]
13. Пациент, у которого был диагностирован коронавирус, прибыл из Парижа в Ташкент 11 марта // <https://kun.uz/ru/47409546> Pacient, u kotorogo byl diagnostirovan koronavirus, pribyl iz Parizha v Tashkent 11 marta // <https://kun.uz/ru/47409546> (InRuss)]
14. Совместное заявление о защите данных и неприкосновенности частной жизни в условиях борьбы с COVID-19// <https://www.un.org/ru/coronavirus/joint-statement-data-protection-and-privacy-covid-19-response> [Sovmestnoe zayavlenie o zashchite dannyh i neprikosnovennosti chastnoj zhizni v usloviyah bor'by s COVID-19 // <https://www.un.org/ru/coronavirus/joint-statement-data-protection-and-privacy-covid-19-response> (InRuss)]
15. Закон Республики Узбекистан «О персональных данных» // <https://lex.uz/docs/4396428> [Zakon Respubliki Uzbekistan «O personal'nyh dannyh» // <https://lex.uz/docs/4396428> (InRuss)]

УДК: 617.571-007-089-053.2

НАШ ОПЫТ ХИРУРГИЧЕСКОГО ЛЕЧЕНИЯ ВРОЖДЕННОГО ВОЗВЫШЕНИЯ ЛОПАТКИ У ДЕТЕЙ РАННЕГО ВОЗРАСТА

Джураев А.М., Усманов Ш.У., Рахматуллаев Х.Р. Халимов Р.Дж.

**ГУ.Республиканский специализированный научно-практический
медицинский центр травматологии и ортопедии, Ташкент**

Врожденная высокая деформация лопатки, широко известная как деформация Шпренгеля, редкая врожденная деформация неизвестной этиологии возникает из-за прерывания каудальной миграции лопатки в раннее развитие плода, приводящее к приподнятой и гипоплазированной лопатке. Оставленная без лечения деформация Шпренгеля часто приводит к функциональным и косметическим нарушениям, таким как ограничение движений плеча и выраженная ипсилатеральная перепонка шеи.

В данной работе мы представляем несколько клинических случаев лечения детей с деформацией Шпренгеля, где рекомендовано при планировании хирургической коррекции врожденного высокого стояния лопаточной кости необходимо учитывать высоту расположения лопатки, сопутствующие изменения в костях грудной клетки, позвоночника, патологические изменения формы и размеров лопаточной кости. А при наличии деформации формы лопаточной кости после полной мобилизации лопатки целесообразно полная коррекция патологической формы для достижения равномерного прилегания ее к поверхности грудной клетки и равномерного скольжения при движениях верхней конечности.