

Медицинские данные порядка 4 тыс пациентов Мичиганского университета здравоохранения (University of Michigan Health Systems, UMHS) были скомпрометированы после того, как в прошлом месяце было похищено больничное оборудование из автомобиля поставщика лекарственных препаратов. Поставщик лекарственных препаратов, калифорнийская компания Omnicell, признала, что нарушила нормы хранения персональных данных пациентов, когда оставила записи о назначенных лекарствах и режиме их приема в устройстве, которое было похищено из автомобиля сотрудника компании.

К счастью, похищенные данные не содержали ни адресов пациентов, ни телефонных номеров, ни номеров социального страхования. В начале прошлой недели пострадавшие пациенты были уведомлены о случившемся. Отметим, что кража данных пациентов UMHS является не единственным случаем в длинном ряду нарушений безопасности, в результате которых были украдены устройства или диски, содержащие данные пациента.

Вчера газета Washington Post опубликовала доклад, касающийся проблем компьютерной безопасности сектора здравоохранения, одной из которых является устаревшее программное обеспечение. В докладе говорится, что исследователи безопасности обнаруживают очевидные уязвимости, которые давно эксплуатируются хакерами. Одним из примеров слабой безопасности является тот факт, что медицинский центр университета Чикаго использовал незащищенные учетные записи Dropbox и одинаковые имя пользователя и пароль, используемые для ухода за пациентами через мобильные устройства.

В последнее время риск выходит за рамки кражи личных данных и мошенничества. Доказано, что таким образом можно контролировать инсулиновые помпы и кардиостимуляторы, что, в итоге, может привести к летальному исходу. Источник: securitylab.ru