This document is a comment on the Digital Millennium Copyright Act, Public Law 105-304 (1998), specifically the new Chapter 12 to title 17 United States Code, with special attention to section 1201 provides that "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." It is submitted as solicited

A brief review of the comments posted on the official internet site for the initial public comment period, shows that most of the points I intended have been made, and made well, so in the interests of clarity, I will add only two points that I feel deserve special attention, and which fall into my specific expertise.

I was formerly the Chairman of the Massachusetts Medical Society Committee on Computers in Medicine (later the Committee on Information Technology) and the National Coordinator for the Task Force on Computers in Medicine of AMSA (the American Medical Students Association). Though I no longer represent either of these bodies, my experience in these positions suggest that there is absolutely no question that making access control a matter of 'vendor right' rather than 'user control of data', invites exploitation in ways that are almost impossible for men of good will to conceive.

The Impact of DMCA on Medical Records, Physician Office Management and Patient Care as a Specific Case of a More General Threat

I. Access control of user data

From the time of the first computerized office management systems (through, I imagine, the present), many physicians have found their office billing, scheduling *and patient medical record data* held hostage by the companies that owned the billing system. This data was deliberately stored in a proprietary format to keep it out of the hands of the physician, effectively holding it hostage. If physicians did not renew annual software license and maintenance contracts with their original vendor, they would lose ***access*** to all their data, despite having physical possession of it

The vendor wished to keep the customer, even if the vendor's product did not meet his or her needs; even if licensing fees had become exorbitant; even if another company's product offered improved patient care, better medical record security; etc. One might argue that vendors of inferior software might be *especially* interested in "locking clients into" their product (even if it were buggy or unreliable) to stay in business.

To change to better software, while retaining the existing data (to ensure best medical care), the physician was forced to hire a programmer to convert the data from the vendor's proprietary format to a public one, such a field delimited text. Numerous court cases were fought, where vendors argued that this conversion was a violation of their proprietary rights. I will not review them, because the details varied greatly.

Under DCMA, the physician would have no such recourse. His/Her data would forever be the possession, though not the property, of the original vendor, to be read only under the terms of the vendor.

This is just a specific case of a general evil of DCMA.

This abuse could be generalized to any form of program that manipulates or alters data (e.g. graphics program, database, word processor, audio 'studio' program, etc.) and stores it in a proprietary format. In each of these cases, the data clearly belongs to the user, not the vendor, yet the vendor controls access under DMCA. This is an implicit threat of most 'shrinkwrap licenses', come to life: *"This program is not warranted for suitability for any specific user purpose, or any general purpose, whatsoever."*

When combined with the 'license change' provision of UCITA (below) this creates horrific scenarios.

II. DMCA in conjunction with UCITA

It should also be noted that under the provisions of UCITA (which has already been passed in at least one state, Virginia, and is pending in many others), a vendor may change the terms of licensing, and the new

license would apply to grantees under the old license. **That is to say, that if a vendor license grants certain rights, the license may later be altered, and the granted rights lost.**

Even id a vendor granted usage rights *in perpetuity* (e.g. allowing a physician to use the program to read the data stored in the proprietary format forever), he can now alter the license to revoke that grant. Under UCITA alone, this only prevented the physician from using the licensed program, but under DMCA, it would permanently ban his/her access to the data. In short, the vendor is granted rights. It also means that formats that are licensed for free public use under explicit licenses such as the GPL (Gnu Public License) could be converted to proprietary licenses at some later data. This would be a data boobytrap for even the most conscientious physician seeking to protect his/her access to his/her data.

The very review process to which this comment is being submitted accepts Adobe Acrobat, Microsoft Word 7.0 or older, Rich Text Format (RTF) submissions as MIME attachments, but not a plain text e-mail. Please be warned that if DMCA were in effect, and this comment were initially read in a Virginia office, the owner of these file format could alter their license to deny you the right to open this document, to convert it to another format, or perhaps even to transmit it to another jurisdiction like DC, where the 'access control' could be circumvented. They could even argue that hardcopy created with their word processor, and without their express license (revocable at their will, under UCITA) is a violation.

Today, few documents are created by hand or manual typewriter from inception to final form. Access control can become very effective censorship on any subject.

Companies will ***and do*** censor criticism. Earlier this week, Mattel used DMCA to block distribution of a free program that allowed users to see data (stored on their own hard drive) which revealed that a Mattel consumer software program did not function effectively at its intended purpose. Mattel obtained an injunction on the basis that that data was stored in a file on the user's computer in a proprietary format, and acknowledged that it would harm their business if users could read it.

Access control can also be used to co-opt the property rights of any user. Most major graphics, audio, and work processing programs are stored in a proprietary file during the work process of creating a work, and only converted to exportable 'open' form on request. Under DMCA (especially in a UCITA state) any such program could begin to charge me fees to export, distribute or use my own work product.

I have heard testimony from physicians whose data has been held hostage, and read accounts of many more cases. Medical software vendors *who invariably advertises the life-saving benefits of instant access to patient data* will lock data knowing the effects are potentially lethal (in an ER there may be only minutes to determine previous drug reactions, allergies, and medical history). Put bluntly, though I know of no specific cases, it is easy to see that deaths may already have occurred due to this practice.

I think it is clear that less dramatic abuses of the principle of 'access control' will be the rule, rather than the exception. Why would it not? Access Control will be a legal right, arguably not an abuse at all.

CONCLUSION:
I could say far more, but I only learned this after noon these are the final hours of the open comment period. Please do not think this provision of DMCA is simply about CDs and pirated videotapes. Its consequences could reach deep into you own family at any time, with tragic results.

Freedom of information is among the founding liberties of this nation, and rightfully so. When access to information is controlled, much else is controlled besides. We must act with utmost caution in this area.

Soumen Nandy
30 Selfridge Road
Bedford, MA 01730

(781)275-3402 phone