Duke University Medical Center Library & Archives
Policy: Privacy Policy
Policy Number: ADM-15
Effective Date: February 2006
Revision: May 2008, December 2013

General Statement

The overarching goal of the Medical Center Library & Archives (MCL&A) is to respect each user's right to freely access information and to protect the privacy of the patron in terms of the information that is used or accessed.

In achieving this goal, MCL&A strives to collect the minimum amount of information required to deliver services or resources to the user. When such information is collected it is treated as confidential private business records and is not available or released to individuals not employed by the MCL&A unless through a legal court order.

MCL&A business records are destroyed as soon as feasible according to standard business practices or legal rules, as in the case of the copyright law.

Circulation Records

The online circulation system contains a record for each patron with basic information about his or her university status as well as campus and home addresses and phone numbers. Only MCL&A staff has access to these records and may only access these records for legitimate business purposes.

The system only maintains a record of what each patron currently has checked out. No records of prior loans are retained by the system; the borrower's information is separated from the item borrowed. Under NC State Law the confidentiality of these resources is protected. MCL&A staff cannot tell other patrons or staff who has certain library material checked out or what a patron has currently borrowed. However, records can be released to state or federal authorities with the appropriate legal court order.

Once materials are returned, all links between the borrower and materials are erased and it is not possible to track what a patron has borrowed in the past.

Archives User Records

Materials in the Archives are at risk for theft, damage, mutilation or loss. Due to these unique security concerns, records of patron use of materials must be kept for several years. Archives will retain all user records, which include the researcher's name and materials used, for 5 years. After five years the records will be destroyed.

Website Logs

MCL&A does track the use of its Web pages, including the IP address of the user. However, no other user information is collected such as the email address, etc. The data is used to analyze the Website as well as for university security purposes. Since Duke's IP addresses are dynamically assigned by the DHCP server, it is difficult to track usage to a specific machine or user. When the data is analyzed it is done in the aggregate and individual IP addresses are not analyzed. This data is destroyed after two years.

Computer Workstations

MCL&A does not track use at individual workstations or retain any logs of use. The cache of the computers is erased on a regular basis. MCL&A blocks storage of personal files on its public workstations and asks patrons to save files on media, which belongs to the patron. No email accounts or files are maintained on public workstations. Information Technology Services does clean off head-drives on a regular basis in case extraneous files are saved. All old workstations are disposed of according to Duke policy so that hard drives are completely erased.

Ovid Accounts

Personal Ovid accounts are maintained by the Library to provide access to features and functions only available through individual passwords. The Library does not track individual use. It does track use by department and discipline, but only aggregate data are collected.

The use of personal passwords, as opposed to generic passwords, does allow tracking of the searches performed by an individual. This data is held by Ovid Technologies and is not routinely released nor routinely erased. The Library does not maintain or track data by individuals, but with a legal court order the government through the police or other federal agency can request that data from the Library and directly from Ovid.

Interlibrary Loan and Photocopy Requests

The Library is required under the US Copyright Law to maintain records of all interlibrary loans obtained from other libraries as well as any photocopies made for faculty, staff or students. The requestor's name is retained on these records, which must be kept for three years after the request is filled. The Library routinely destroys these records once the three-year period has expired.

Bills and Invoices

The MCL&A must retain all financial records for 5 to 7 years, depending on the type of record. These documents do contain patron names and the services delivered to them. The MCL&A destroys these records as soon as Duke financial policies allow.

Surveys and Prize Drawings

The MCL&A occasionally has activities when a patron may decide to identify themselves.

Surveys conducted by MCL&A are usually anonymous and data analysis is done on the aggregate level. IP addresses may be collected as part of the survey data, but these are not analyzed or linked with the responses. Sometimes a survey will provide the option for you to leave your name and contact information, if you want a response to a comment or receive the results of a survey. Again, this information is kept confidential, is not linked to the responses, and destroyed at the end of the data analysis.

Prize drawings are held around special events or in conjunction with surveys. The user voluntarily agrees to share their name and contact information. However, once the drawing is completed, all user records are destroyed.

VPN/Net ID Accounts

The VPN and NetID accounts are used to access Duke resources. However, MCL&A does not provide and is not responsible for the use of these systems. If you are concerned about privacy should contact DHTS regarding their Health System VPN accounts and OIT for the privacy of NetIDs and University VPN accounts.

Monitoring of Unauthorized Use of Licensed Resources

Publishers of databases and online journals require that the MCL&A monitor access for unauthorized use, such as a non-Duke person using a Duke account to access databases, e-books, etc. The MCL&A may track usage if it suspects that unauthorized or illegal use is occurring. This information is kept confidential and only shared with Duke's IT security officers.

Publishers also track usage and will report suspicious use that may be violating contracts, such as unusual IP addresses or substantial downloads of data, book chapters, or journal articles. They usual provide an IP or email address. When this occurs the MCL&A has a formal protocol it follows, first trying to establish the identity of the user and then contacting the user directly to see if the use is legal within the terms of the license. The University IT security offices may be brought in if identification is difficult or the problems persist. All information regarding the user's identify is kept confidential. User accounts may be cancelled temporarily or permanently depending on whether the user can be identified and contacted, if they are an authorized Duke user, and the nature of the activity.

Privacy of Other Computer Systems

Most commercial computer systems track usage and patrons need to be aware that government authorities with a legal court order can request the release of any information stored on the computer regarding the use of resources or communications with other people.

The MCL&A can only guarantee privacy for the workstations within its facilities. If a patron connects to another server or workstation, or uses an online service or e-mail, there is no way

that the MLC&A can guarantee the security and confidentiality of the data. E-mail and other systems routinely maintain backups and if you are concerned about your privacy you may wish to contact those services about their privacy and security policies.

Most vendors and publishers of electronic resources track usage by IP address and have records that connect specific IP addresses (computers or wireless nodes) to the resources used. Those vendors that provide password access, such as MD Consult, also track individual users and also have records regarding individual use. In the general contracts, the Library requires that the vendor keep the information confidential, uses the information only for internal evaluation and marketing decisions, and publicly reports any data in aggregate form (no identification of specific users). However, that data is still available from the vendor, and with a legal court order, can be turned over to government authorities during an investigation.