United States Masters Swimming
Data Base Project Privacy/Security Subcommittee

Introduction

USMS maintains a number of databases containing information about its members, past and present, as well as their activities such as competitive results and organizational meetings. It is likely, as computer technology and connectivity continues to evolve, that USMS will add to the list of databases it uses. As part of a project to improve the database systems, the Privacy/Security Subcommittee proposes a policy that will define access to and security of USMS databases.

Mission Statement

The Purposes of the Privacy/Security Subcommittee are to:

1. Determine what data needs privacy protection;
2. Determine and propose who should have access to data;
3. Determine and propose the data to which identified categories of persons should have access; and
4. Identify USMS needs with regard to keeping that server secure from intrusion.

Mission Objectives

1. The subcommittee will provide information in order to fulfill the USMS Database Project mission objective to ensure that the "system shall be designed to protect the privacy of members and users."
2. The subcommittee will provide information in order to fulfill the USMS Database Project mission objective to ensure that the "system shall be designed so it contains features to maintain the security of the information maintained in the databases."
3. The subcommittee will propose what data should be available for public view on the web site.
4. The subcommittee will propose what data should be available for view on the web site through a restricted access system (by pass code or through the National Office).
5. The subcommittee will propose which categories of users will have access to information through the restricted access system and what specific information should be available to each category of user.

Data

USMS assembles data about its members for various reasons. The data is stored in a number of formats both computerized and manual. While the means of protecting the privacy of the information contained in these databases will be dependent upon their form, the need to do so is not. For example, data that is deemed private needs to be equally protected if it is contained in a database on a computer or is in a report printed out from that database. An understanding of what information USMS maintains and how it is used leads us to an understanding of the privacy we can afford the data.

The types of data held within the current or proposed USMS databases can be broken into two broad categories: biographical and participatory data. The biographical data includes the information that can be used to identify a person such as name, date of birth, gender (see below for a more complete list). The participatory data is that data that describes the activities of the members both past and present. This category contains all of our competitive results but could also include data about organization information such as committee membership, committee meetings and the like. Separation of the data into these two categories simplifies the discussion of access to the data by various individual and groups both internal and external to USMS.

The latter category, participatory data, by its very nature is public with very few exceptions (for example, disciplinary hearings). Therefore, excluding the few exceptions, the participatory data should be public data which anyone, member or not, can view. Thus if a member enters a swimming meet, the results of the events contested will become part of our public record. An individual entering a meet should understand that all of the information necessary to define the results would be public. Thus the individual’s name, age, gender and club membership as well as the fact that they participated in a given meet is public and will not be protected from disclosure.

The protection of an individual’s biographical data is a more difficult issue complicated by the fact that different individuals and groups within USMS need varying access to portions of the data. This committee recommends various levels of access based upon need and recognizes both continuing as well as temporary access to member's personal data. The details of that access policy are described in the remainder of this document.

Access Control

The most sensitive access issue is, of course, access to personal data and this document will primarily deal with that issue. There should be four different categories of access to specific information about individuals: routine access, restricted access, restricted access through the National Office only, and no access. In addition, access to bulk information through mass search should also be restricted. Access to all biographical data should be denied to the general membership (and the public) since there is no routine need for the data. Routine access should be granted to those individuals who, in order to conduct their routine daily business for the organization need access to the specific data. Restricted access to the membership biographical data or a subset should be granted by an authority (for example, the House of Delegates or the Executive Committee) to an individual or committee on an as-needed basis. The restricted access should be specific with respect to the type of data as well as the duration of access.

The form of the access will be dependent upon both the nature of the need as well as the current state of the database. Each type of access should have a controlling mechanism (password, delivery by e-mail of password protected files, delivery by USPS mail) to provide security for the data and is considered an implementation detail specific to the database.

Specific Access Recommendations

Appendix A - Matrix of Data Access shows a comprehensive list of what data *might* be accessible by various persons. Appendix B - Tables of Information shows all the categories of users and data under consideration. Using this information as a basis for discussion, the subcommittee recommends the following access rules:

1. For Performance Data, the public will have access to the data mentioned on the matrix and mass search will be allowed.
2. For USMS Position Holders in their Official Capacity, the public will have access to the data mentioned on the matrix and mass search will be allowed.
3. For general membership biographical information, the subcommittee has identified a limited number of users who need access for the day-to-day operations of USMS. The subcommittee recommends giving permanent access to LMSC Registrars, National Office Workers (at least Executive Secretary and Data Base Administrator), Records & TT, History & Archives, and IT Employees. The Executive Committee, as final authority on who gets access, should also be included. The level and content of access will be as represented on the matrix and mass search will be allowed. All other entities will get access for limited purposes when they need it, either directly or through requests to the National Office.
4. Meet directors should have access to the biographical data shown on the matrix with the following restrictions: a) access shall be for a limited time period and contingent on the meet being sanctioned or recognized; b) meet directors shall only have access to information one person at a time and shall not have the ability to do a mass search; and c) meet directors must sign and return the USMS database access policy (see Business Rules below).

Special Considerations

Access to biographical data at the local level warrants additional discussion. Within the normal conduct of business, clubs or LMSCs may find it desirable or necessary to make available to their members rosters that contain biographical data such as address, phone numbers and even birth dates. The reasons for disclosing this data can vary from the need to foster participation in relays to facilitating communications among members (e.g. phone trees for practice groups). USMS should make available its privacy policy to each LMSC and encourage each to at least follow the spirit of the USMS policy while acknowledging the needs of the local organizations.

USMS, may on occasion, conduct financial transactions with members through the use of credit cards. USMS should retain the credit card information in encrypted form in a separate file only for the time necessary to complete and verify the transaction with its credit card clearing house. USMS should not maintain any permanent record of credit card numbers.

The subcommittee discussions have ranged beyond data which will be contained in the proposed on-line database as well as the privacy that should be afforded to data which is protected by this policy but which is no longer on-line (e.g. it has been printed out in a report) or which has been collected by other means (e.g. a meet director's access to birth dates). We recognize that these data are not part of the charge to the subcommittee, but they are of concern to the privacy issue in general. Either the database committee as a whole, or a standing committee (by way of an action item for convention) should refer to another committee (e.g. Legal Counselors) or the Executive Committee, a request that a global privacy policy be developed for USMS to cover all forms of arguably private information that USMS collects.

Business Rules Governing Access

It is recommended that USMS institute the following business rules governing access to data that include:

1. The return by each person granted access of a signed copy of the USMS database access policy acknowledging the policy prior to being granted access.
2. Granting access to users at a level commensurate with their highest position in USMS.
3. Specification that regardless of the level of access granted, use of data shall not exceed the level of the job for which it is obtained.
4. A denial of access to the USMS databases for any users found to be obtaining data for improper uses. The period of the suspension shall be determined by the Executive Committee.

Security

In order for the above principles and rules to have the desired effect, the various databases held by USMS should be maintained in a secure environment. Databases maintained on computers connected to the Internet must use the best available practical means of protecting the data from unauthorized access including both viewing and alteration. Databases held in non-Internet connected environments must also be secure from inadvertent disclosure based upon the form of the database.

Appendix A - Matrix of Data Access

Individual Data	**ACCESS KEY** **Blank = no access** **A = available** **R = restricted** **N/O = National Office Access** **N/A = Not Applicable**	General membership	Registrars in same LMSC	Registrars in other LMSC	LMSC Chair or designee in same LMSC	Meet Directors	National Office Workers	Records and TT Tabulators	History and Archives	Board of Directors	Executive Committee	House of Delegates	USMS Committee Chair or designee	Sponsors Researchers	IT Employees	Special assignments	On-line registration if available
Biographical	***General members***																
	Name		A	A	A	A	A	A	A	A	A	A	A	N/O	A	A	A
	Address		A		A	A	A				A		R	N/O	A	R	A
	Gender		A	A	A	A	A	A	A	A	A	A	A		A	A	A
	DOB		A		A	A	A	A	A		A		R		A	R	A
	Club		A	A	A	A	A	A	A	A	A	A	A		A	A	A
	E-mail		A		A	A	A				A		R		A	R	A
	Phone		A		A	A	A				A		R		A	R	A
	Registration number		A	A	A	A	A	A	A	A	A	A	A		A	R	A
	Credit Card																A
	Available through Mass Search		A		A		A	A	A		A		R	N/O	A	R	A
Performance																	
	Name	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	N/A
	Meets	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	N/A
	Event results	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	N/A
	Age	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	N/A
	Club	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	N/A
	Available through Mass Search	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	N/A
Biographical	***USMS Position Holders Acting in Their Official Positions***																
	Name	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	N/A
	Address	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	N/A
	E-mail	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	N/A
	Phone	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	N/A
	Position in USMS	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	N/A
	Available through Mass Search	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	N/A

Appendix B - Tables of Information

Categories of Users	
National USMS Officials	
Executive Committee	
USMS Board of Directors	
National Office personnel	
Standing Committee Chairs	
Ad-hoc Committee Chairs	
Records & Tabulations	
History & Archives	
Special Assignments	
House of Delegates	
National Championship Meet Directors	
Other Database Owners	Access to be determined on a case-by-case basis
On-line Registration (if available)	
Local USMS Officials	
General Membership	
Registrars working in same LMSC	
Registrars in other LMSCs	
LMSC Officers in same LMSC	
LMSC Officers in other LMSC	
Meet Directors	
Non-USMS Officials (Can be USMS Members working in a Non-USMS Member Capacity)	
Liaisons to USMS BOD	
Researchers	
Sponsors	
Web Site Developers (Can be USMS Members or Non-USMS Members)	
Contractors	
IT Employees	
Web Site Administrators	
Web Site Workers	

Data Needing Privacy Protection	
Name	
Address	
Gender	
Date of birth	
Club	
Email address	
Telephone number	
USMS Registration Number	
Credit card information	Credit card information to remain in the system only long enough to be cleared
Medical information	
Email lists	
Registration history	

Data Needing Security Protection	
Credit card information	Credit card information to remain in the system only long enough to be cleared
Birth date	
Passport Number	