Data Governance

- Intro to data governance
- link to EDA resources
- link to data governance
- **Enterprise Data Governance**
- **Data Governance Council**

Data Governance for Humanitarian Services

Data governance includes standards for collecting, managing and storing data. It also encompasses retention, destruction and processes and controls for sharing records.

Data Sharing

In an effort to increase effective data sharing, Humanitarian Services has created guidelines on data sharing. The following policy guidelines seek to ensure that as an organization, data is shared in an effective way possible. Part of this governance includes access controls on certain record types, while making others more widely available.

Resources:

This guidance document is a supplement to the policy resources below, in order to better reach HS system owners and users on HS specific guidance on data sharing. Please, refer to these policies for organization-wide procedures.

Standard – Data Classification and IT Solution Categorization

Protecting Personal Information Policy

Records Management Policy

Classifications

Data sharing questions on a larger scale ask if sharing certain data is ethical, safe, and useful. The same approach is applied to data within Humanitarian Services systems. Before data is shared across systems to users, owners the data should consider the following as outlined by the office of Information Security: the confidentiality, integrity and availability of the records. If the records were disclosed to unauthorized users, or modified, would this have serious consequences on the operations or the departmental/organizational assets.

PII

Personal Identification Information is one bucket of data that should be treated with high confidentiality. This data should be shared only with users given permissions to access the data. Authorized users can include volunteer and staff who need to use the data for business purposes. Sharing of this data should follow ARC standards and security measures of handling PII data, see Information Security Policy for more information. Please refer to Use of Data' section below for the specifics of using PII under the data sharing agreement.

Access

Controls on the type of data that is available for usage is a key tool in ensuring data sharing allows for organizational effectiveness while remaining safe and conscious of the risks associated with this. This means identifying the type of users that can have access to highly confidential data and restricting that data to all users who do not fit the requirements. System owners should identify which records are considered confidential and which is official use by redcross.org users. Please refer to the Data Classification and IT Solution Categorization to better understand these standards.

Security and Sharing

It is important to consider generic security measures when sharing data with authorized users and colleagues. First, ensure that information is never shared through vulnerable means. Classified information should not be shared through an email attachment, as leaves our data vulnerable to hackers. Email attachments can be downloaded and saved which may also disrupt data retention policies. Instead, consider using internal reporting dashboards and other secure and private approaches. SharePoint sites with classified data should utilize privacy options. Owners of SharePoint site can ensure only a select group of people can view and edit information on the site. This prevents data being shared to staff and volunteers across the organization.

Data Usage Agreement

A data use agreement establishes who is permitted to use and receive the data, and the permitted uses and disclosures of such information by the recipient and provides that the recipient will follow the Humanitarian Services' data usage. By accessing Humanitarian Services data, you are agreeing to the policies outlined.

Modification of this Agreement

This policy document is living and is subject to change as sharing policy standards update, means of access develop, and business needs evolve.

Use of the Data

Use of the data includes but is not limited to accessing, viewing or the whole of the content included in the comparing data or content from the materials with data or content in other materials; verifying analytical results with the content included in the data; and extracting and/or appropriating any part of the content included in the data for use in other projects, analysis, reporting, or other related work products. Parties that request and/or have existing access to HS data must agree to the terms below.

1. User will not utilize the data in any way prohibited by applicable IT security policies.
2. User will not store or share data beyond the means of business needs and will not release PII or any additional information that could be linked to an individual, nor will the recipient release the results of the data analysis in any manner that would reveal the identity of individuals or other classified information.
3. Data and analytical analysis from data will not shared with authorized users beyond the scope of safe means outlined in IT security policies, i.e. data will not be shared via email without encryption.
4. Data will not be shared with any third party without explicit consent from the data owner.
    a. Any third party that is granted access to the data shall be subject to the terms outlined in this agreement.
    b. Third parties with access to data should have review HS Data Sharing Policies outlined in this document.
5. Data integrity will be observed, and users will not alter data in means beyond what is authorized when accessing, storing, and processing.

Data Owners are responsible for system adherence of data sharing policies and for approving and/or delegating responsibilities to approve of access of data. Owners can reach out to HS BSI Decision Support team with any questions regarding access.

Compliance

Users of data should have safeguards in place in order to protect HS data. These safeguards can be the following: administrative, meaning a set of requirements users meet to be gives access to the data, policies and procedures in regard to data collection methods, use and disclosure of data; technical meaning not sharing data through unsafe means, such as sharing data through email attachments without encryption and locking your computer screen when not in use; and physical safeguards. While having physical copies of records is not recommended, if there is a business need, ensure the records are kept in a safe and secure location. For more information on this matter, refer to the Information Security Policy, Procedures, Standards and Guidelines Updates toolkit.

Record Retention and Destruction

The purpose of this document is to outline and define the guidelines in which records should be stored, for how long and the processes for destruction of these records. As Humanitarian services collect and store various kinds of records, having a common policy that includes high to low confidentiality and high to low available data. Please refer to Records Retention and Destruction Procedure established by the Corporate Secretary's office.

One of the main objectives in section 4.1 of the American Red Cross Records Management Policy is to "(e)ensure records and other documents are retained for a period of time that will reasonably assure their availability when needed, but not longer than reasonably necessary." Section 4.2.1 of the accompanying Records Retention and Destruction Procedure states that Red Cross units with primary responsibility for Business Records shall:

(1) determine the retention period based on legal requirements or business needs;

(2) establish internal processes for maintaining the records that fall into that category for the retention periods specified; and

(3) ensure compliance with the Records Retention Schedule and the established instructions in this Procedure for records retention and destruction.

Acceptable records destruction protocols

Section 4.6 of the Records Retention and Destruction Procedure states that "(r) ecords that are not required to be kept permanently can be destroyed after they have met their required retention period as indicated in the Records Retention Schedule. This may be accomplished through scheduled, periodic clean-up events or systematic deletions from applications or repositories based on IT policies, standards and procedures. Care should be taken to ensure that all copies of a record are deleted or destroyed."

The following sections outline specific retention policies for the various Humanitarian Services systems, based on the business needs of users, data owners and the clients being services.

Storage and Destruction

Records should only be stored in formats and locations approved by the Data or Product Owner of the various systems and in accordance with IT policies.

All data stored in each identified system must be destroyed within the outlined dates according to the data type.

RC Respond:

Record Type	**Destroy/Delete After**
Call Records x	7 years
Communications	7 years
DAT Activation	7 years
DAT Responder Notes	7 years
DAT Responder Reports	7 years
DAT Responder Status	7 years
DAT Response Log	7 years
DAT Role	7 years
DAT Schedule	7 Years
DRO	7 years
Volunteer Connection Contact	Never/ Archive
Non Volunteer Connection Contact	Never/ Archive
Support Schedule	7 years

Destruction Procedure

The RC Respond contact specifies that data will be destroyed when it is older than 7 years. The Data Owner will confirm that the data is being destroyed per the contract, as part of their quality control spot checks.

RC Care:

Record Type	**Destroy/Delete After**
Active Clients	Never
Inactive Clients	7 years
Active Accounts	Never
Inactive Accounts	7 years
Closed/Inactive Cases	7 years
Active Cases	Never
Financial Assistance	7 years
Uploaded Documents	7 years
SAF Emergency Communication	*12 months*
Inquiries	7 Years
Transaction Logs	7 years
Communication Records	7 years
Inactive Users	7 years
Events with no Cases	7 years

Client Surveys	7 years

Destruction Procedure

1. The Salesforce COE will provide the Product Owner of the RC Care instance and the Data Warehouse team 90 days notice prior to deleting any data.
2. At that time a report of the business records to be deleted will be provided based on the age of the records and the parameters defined in this policy.
3. The Product Owner and Data Warehouse may request exceptions or approve all records for deletion.
4. Once approved, the COE will perform a deletion process in the database.

Definitions of Record Types:

Active Clients: Contact records of people who are actively being served by American Red Cross and possibly receiving assistance.

Inactive Clients: Contact records of people who may have been served by American Red Cross but do not have any known ongoing services to be provided.

Active Accounts: Account (Household name) records of people who are actively being served by American Red Cross and possibly receiving assistance.

Inactive Accounts: Account (Household name) records of people who may have been served by American Red Cross but do not have any known ongoing services to be provided.

Closed/Inactive Cases: Case records which contain details of services to Clients but have been closed due to completion or became Inactive due to non-completion.

Active Cases: Case records which contain details of services to Clients but have been completed or are in a status of waiting for closure.

Financial Assistance: Records pertaining to direct financial assistance to Clients (Disbursements).

Uploaded Documents: Electronic copies of documents provided by clients to validate identity, damage, address, or other personal information in the course of providing services to the client associated to a Case.

Transaction Logs: records of integration calls with external IT systems. Contains transaction success and failure information along with data provided in the integration call.

Communication Records: email, SMS, chat or other electronic correspondence with a client recorded during progression of a Case.

Inactive Users: User (employee, contractor, volunteer) or Client User (community account) system access account which has not been used within the inactivity determination period and has been inactivated.

Events with no Cases: Event records which were created but have no Cases associated with them during the open period of the event.

Client Surveys: records of survey requests and responses completed during the progression of a Case or interaction with a Client.

RC View Layer:

Shelter Data

Record Type	**Destroy/Delete After**
Facility Sites	Never
Shelter Data	Never
Incident DR	7 Years
Opening Inspections	7 Years
Closing Inspections	7 Years
External Accessibility	7 Years
Operational Accessibility	7 Years
Internal Accessibility	7 Years
POC Details	Never

Survey Conductors	Never