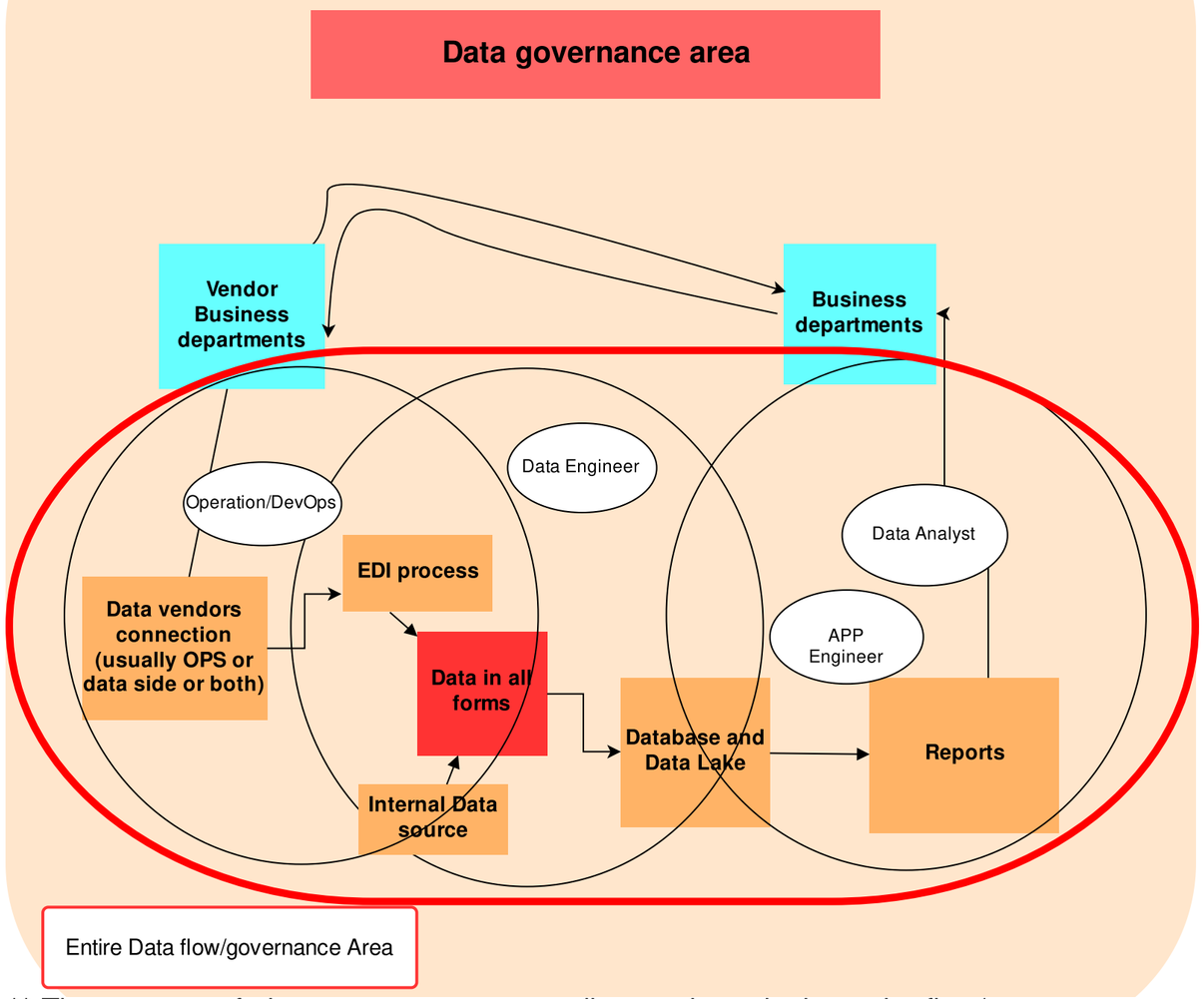
0. Declaration, purpose and scope of Data Governance policy

The purpose of this data governance policy document is to declare data governance and control policy in Centerlight Health System. It is a top view principle that dictates individual and detail rule sets and that every employee of Centerlight Health System must understand and follow.
This data governance policy is the most basic policy over any other policies/rules/documentations in data entire area/flow.

Scope of declaration in Data governance policy: Entire Data Governance Area, Data Governance Structure, Data Access, Data Usage

1. Entire Data Governance Area



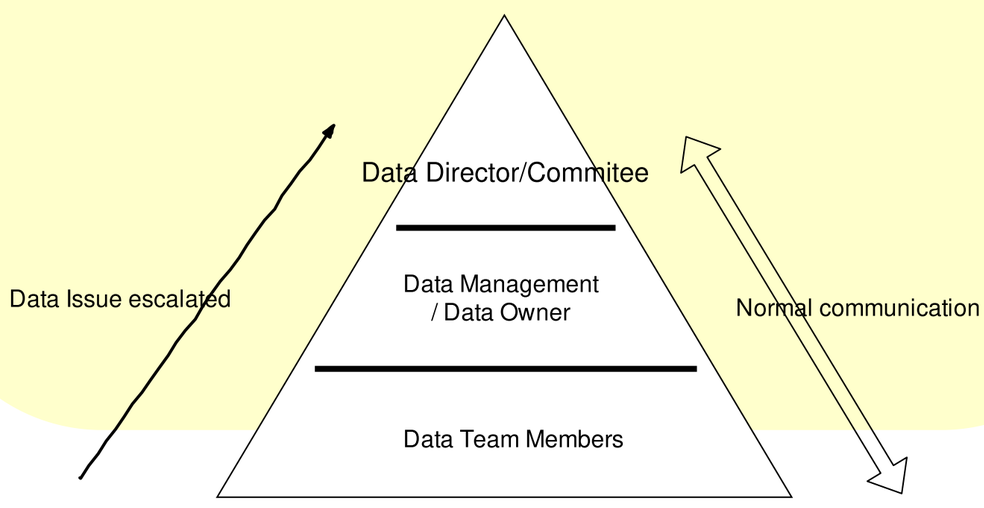
** The purpose of above governance area diagram is to depict entire flow/governance area and general flow. It is not for declaring it is the only flow. Some flow is just internal of Centerlight(internal report requirements, etc.) and some flow is just CL business - vendor business side communication (it could get in the boundary later, of course).

Data governance scope: Data collection, requests, validation, access, consumption, relase, reports. The entire area has connection and interface with business departments' area, so that data team is also engaging with business side to collaborate and make entire data projects successful.

Data team members (in any level) interface and interactions with any other departments (like discussion) must happen in an organized way, meaning not individually random way, which no one else in data team knows kind is not an organized approach.
Rather, Data Director/Data Manager/Data Architect decide what level of engagement/works (for example, one person assignment or project level - design and planning is needed - or multiple assignments (team effort)) are needed.

2. Data Governance Structure

Data Governance consists of the Director of Data, analytics, performance department, the Data Architect, various Enterprise Database teams members/workgroups. Issues are identified and addressed by data team member (Data steward) in the first level. Issues that cannot be resolved by data stewards are escalated up through the data governance structure to the Data Architect and/or Data manger and, if needed, the Director or Director committee. The executive committee meets as needed. Data steward workgroups can be created on an ad hoc basis at the request of individual data team member on discretion by Data Manager or Data Architect.
Everyday and normal communications on any matters of data should be free flow without obstacles and should happen without any delay.
Each relative Department Head gets communication connection route through Data Architect/Data Manager/Data Director so that 'data owners' also get appropriate notifications on data governance area, but It is up to Data Architect/Data Manager/Data Director's decision whether to escalate to that level is appropriate or it is appropriate for just internal data team resolution because some issues are just inside data structure, process, and other kinds of internal issue while other issues are business logic decision involved.



3. Data Access

Data Access level/permission and/or any limitation is determined by DBA or Data architect in accordance with Data director or director committee decisions.
Each detail level of permissions is mainly decided by Data Architect, DBA, Data Manager per each access level requirement. Minimal permission principle is the basic rule - i.e., everyone gets 'necessary' level permission to do one's job/role, not more, not less.

Data Architect, DBA, Data Manager are top level access permission allowed group to Data. i.e., Management and administrator level. However, DBA is technical part of admin level access, therefore, Data contents level is not within DBA role boundary.

Plus, any designated individual by Director/director committee per legal/business requirements will get necessary access permission - for example, third party or state/federal level legal auditor gets necessary access.

Data team members - Data Team Members in this policy does not mean a person has to belong to a formal data process department. It means job role is CL data process related and within data governance scope (at least, a part), thus some outside of formal data department members would be included. Example: Finance department member works on CL database and makes a report out of, then belongs to the definition of data team member in this policy.

Data engineer, Data analyst, Application engineer, Data visualization (BI) and Report developer get contributor (Data read, Data write) permission depends on 'area' or each database requirement for job assignment perspective. Each team or individual permission level is set by Data Architect. However, still minimum permission principle is applied. On the other side, this minimum permission principle also should consider backup purpose roles in case an assigned person is absent. Then, delegated and accelerated permission could be assigned in the meantime.

For outside of data management/analytics team, Centerlight users/staff members (Data user) could get some read permission depends on business needs, but write permission is not given unless there is a special and specific requirement exists.
Clear exceptions to the above no write permission for general Centerlight users are cases that business data process defined in such a way that App (or other similar means) provided to users and user entered data through defined process is written/collected into data repository/database.

Designated data vendors or Centerlight partners could get contributor permission in their own respective data area.

General public has no permission to Centerlight data. However, information of their own data perspective, they are information owners, and thereby all necessary notifications are their rights to know when Centerlight has relative data.

Information itself is a separate concept from Data. Data is built/made by Centerlight data team for Centerlight, thus ownership of data is Centerlight.

Data and database access permission request form will be made by Data Architect under Data

4. Data Usage

Data usage in Centerlight is the sole purpose of meeting Centerlight business or legal requirements. No personal usage and any other purpose usage is prohibited.
As security policy states authorized users (all including Admin) must maintain/follow security policy and guidelines to protect authentication/authorization (such as password protection) of Centerlight data.
Anyone in Centerlight who fails on their due diligence of protecting Centerlight data will have consequences of Centerlight disciplinary actions and/or legal consequences.