0. Declaration, purpose, scope, objectives, definition of Data Access/Permission/Authorization policy

The purpose of this data access, permission, authorization policy document is to declare grant and revoke access to Centerlight data within Data governance area of Centerlight Health System.

This policy is intended to supplement Data Governance policy with more details for specifically Data Access, Permission, Authorization area. Thus, this and Data Governance, Data Security policies help one another to build entire Centerlight data policies.

Within its scope, it is a set of top view principles that dictates individual and detail rule sets and that every employee of Centerlight Health System and other persons authorized to use/access Centerlight data must understand and follow.

In this policy, there are below sections:
Access/Permission/Authorization details
Digital Data access/permission/authorization decision tree structure
Enforcement and Regular audit on access
Supplemental Access/permission/authorization request form

Definition:
- Data
Data here means digital data such as Database as a first line, but entire data flow pieces or entirety of information governed by Data governance policy is data regardless of forms (file, text, database, storage, etc.)
- Data engineer
Data engineers are Centerlight employee whose job is to manage/wrangle/organize digital data in Centerlight.
- Data Analyst, Report developer
Data Analysts/reporters are Centerlight employees whose job is to create analyzed output from raw or first source data and produce reports with Centerlight data.
- APP engineers
APP engineers are developing Application and related services in Centerlight. By nature of data flow, an APP engineer more than likely handles data (storage, file or database).
- Data team members
Regardless of Departments and whether a person belongs to a formal Database team or not, digital data handling as a part of job in Centerlight (example: Finance making reports from database) falls in 'Data team' categorization in this policy.
- Data users
Outside of directly dealing with Data, some users fall in Data user category. Data User means any individual who has been authorized to access Centerlight data but does not belong to Data team categorization.
- Data Access/permission/Authorization decision maker
Such decision maker is Data Architect, Data Manager, Data Director under data decision tree governed by Data Governance policy.

1. Access/Permission/Authorization details

1.1 Data Architect/Data Manager/Data Director under data decision tree decides procedures for Requesting, Approving, and Revoking Access
With supplemental Data Access form, Data Architect/Data Manager (DBA, Security specialist could have input on this) will decide final user/group access and permission levels to Centerlight data.

Data Architect/Data Manager/Security Specialist also makes procedures for regularly auditing access to Centerlight data.
They also can and will revoke access when it is no longer needed or authorized.
Either the case of inclusion (like new hire) or revocation (like employee left Centerlight or no longer job role assigned for data access), Data Architect/Data Manager retains full control and any relative assignment such as windows individual/group ID removal decision, and that belongs to Data Architect/Data Manager if/when that is necessary to control Centerlight digital data access because that is directly tied to digital data access.

Each procedure or daily work varies by nature of work, but all access related procedures will include sufficient tracking for requests, approvals and revocations.

1.2 Only Authorized Users will be allowed to access Centerlight data

All access by individuals to Centerlight Data shall be controlled by reasonable measures to prevent access by unauthorized users.

1.3 All Data Users must use Centerlight data responsibly

As stated by Data Governance policy, Data Users must responsibly use data for which they have access including only using the data for its intended purpose and respecting privacy, rules and regulations. Data Architect/Data Manager retains the right to approve, revoke access to sensitive data.

1.4 Data Architect may delegate Approval Responsibilities to a Trusted Designee

When Centerlight has appropriate and designated employee such as Sr. DBA or Data Security specialist, Data Architect may delegate ability to approve access/permission/authorization responsibility for Centerlight Data to such trusted individuals in designated roles. Data Architect/Data Manager retains the responsibility for ensuring that all access to Centerlight Data is authorized, appropriate, and complies with relevant legal requirements.

1.5 External Third-Party or legal auditor Access to Centerlight Data will be governed by Contractual agreement or legal obligation as stated in Data governance policy.

1.6 Data engineer
Data engineers are required to work with raw data by nature of work, thus, Data engineers will have near full access and control of digital data in Centerlight.
However, depends on skill level, and difference in SR and JR level works, Data Architect/Data Manager can decide to give different access level to different groups of Data Engineers.

1.7 Data Analyst, Report developer and APP engineer
They do normal data usage works and, in many cases, work closely with data engineers. Within work range, they can/will have more access permission than normal data users. This kind of individual or group level access will be still decided by Data Architect/Data Manager.

1.8 Data team members
the same responsibilities that apply to formal data team also apply. Authorization level will be decided by Data Architect/Data Manager.

2. Digital Data access/permission/authorization decision tree structure

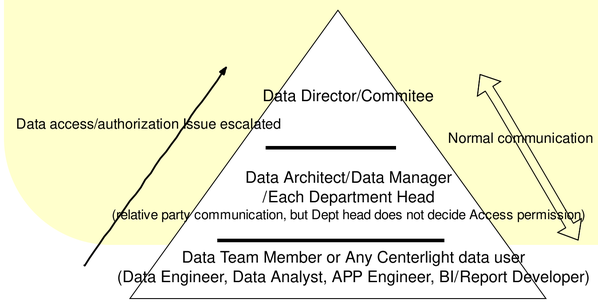
As defined by Data Governance policy, involved parties consist of the Director of Data, analytics, performance department, the Data Manager, the Data Architect, a various Enterprise Database teams member/workgroups.

Regardless of who in Centerlight got requests from potential data user (example: new finance hire needs database access), it must be forwarded to access decision maker (Data manager, Data Architect in first, then maybe chain up to Data director level or delegated person depends on judgement)

Data Access/Permission/Authorization decision belongs to decision maker in this policy, as such, Outside employees of data decision tree on data governance has no right to make Data Access/Permission/Authorization decision.

In essence, Data Access/Permission/Authorization decision flow is simple. Any entity/individual in Centerlight that wants to access and get authorization make contact with Data Manager/Data Architect/Security specialist and if some other entity got requests, regardless of who got contact, immediately forward to Decision maker defined in this policy. Once received by Decision maker, final decision (with possible discussion) is notified to original entity/individual and appropriate permission will be set up by Data Manager/Data Architect/DBA/IT.

When appropriate setup is required, Decision maker will notify IT to set up appropriate windows ID (individual or group) - either new/update/delete - or actions accordingly. these actions may include any actions in data area governed by Data governance policy.
At the same time, Decision maker also will notify Database Administrator or delegated person who is eligible to do so, to set up/update/delete Database level permissions.



3. Enforcement and Regular Audit on Access

Data Access/Permission/Authorization Enforcment is managed by Data Manager/Data Architect on top view.

Any Data Access/Permission/Authorization or such approval, change or termination by not following this policy could be consequences.

Regular audit on Access/Permission/Authorization will be conducted by Data Architect, Data Manager, Security specialist on data access at minimum yearly. All the users/groups/service accounts are audit targets and appropriateness, proper level of authorization, following principle of minimum authorization are all required methods/measures of the audit. Audit conductor can be designated by Data Manager/Data Director/Data Architect. Audit result will be reported to Data Director and appropriate action can be done if/when such action is needed like account access termination.

4. supplemental Access/permission/authorization request form - below is just to show what form actually looks like.
Real request form will be uploaded to Centerlight repository storage area and will be allowed to be accessed by all Centerlight employees.

Person	ID	Department	DB name	Permission	RequestDate	Requestor	General description	DecisionByArchitect	DecisionDate	UpdateDate	UpdateBy	Group
Jin Hyo Ju	[CENTERLIGHT\123456]	Performance improvement	EDW	read	8/17/2023	vhormaza@centerlight.org	need to read tables of member info					
Jin Hyo Ju	[CENTERLIGHT\123456]	Performance improvement	EDWSTG	read, execute proc	8/17/2023	vhormaza@centerlight.org	need to read tables of some claim data tables, and execute a few FIN schema procedures					
Jin Hyo Ju	[CENTERLIGHT\123456]	Performance improvement	CareCompass_Centerlight_Repl	read	8/17/2023	vhormaza@centerlight.org	need to read tables of CC info related to member, claim					
Jin Hyo Ju	[CENTERLIGHT\123456]	Performance improvement	Reports	read, write	8/17/2023	vhormaza@centerlight.org	read and write for finance tables, and views, but no execute proc needed					