0. Declaration, purpose, scope, objectives of Data Security policy

The purpose of this data security policy document is to declare data security and protection policy in Centerlight Health System.
As will be stated in the three entities of data security in Centerlight, the scope of security policy is digital data security policy, therefore, not including other types within scope such as paper, email, network, talks, etc. This means, this policy and other policies will supplement and help each other to build entire organizational data security policies.

Within its scope, it is top view principle that dictates individual and detail rule sets and that every employee of Centerlight Health System and other persons authorized to use
Centerlight facilities/devices must understand and follow.
Data in this policy means, regardless of forms, Centerlight collected, organized, created, consumed data defined by Centerlight Data Governance policy.

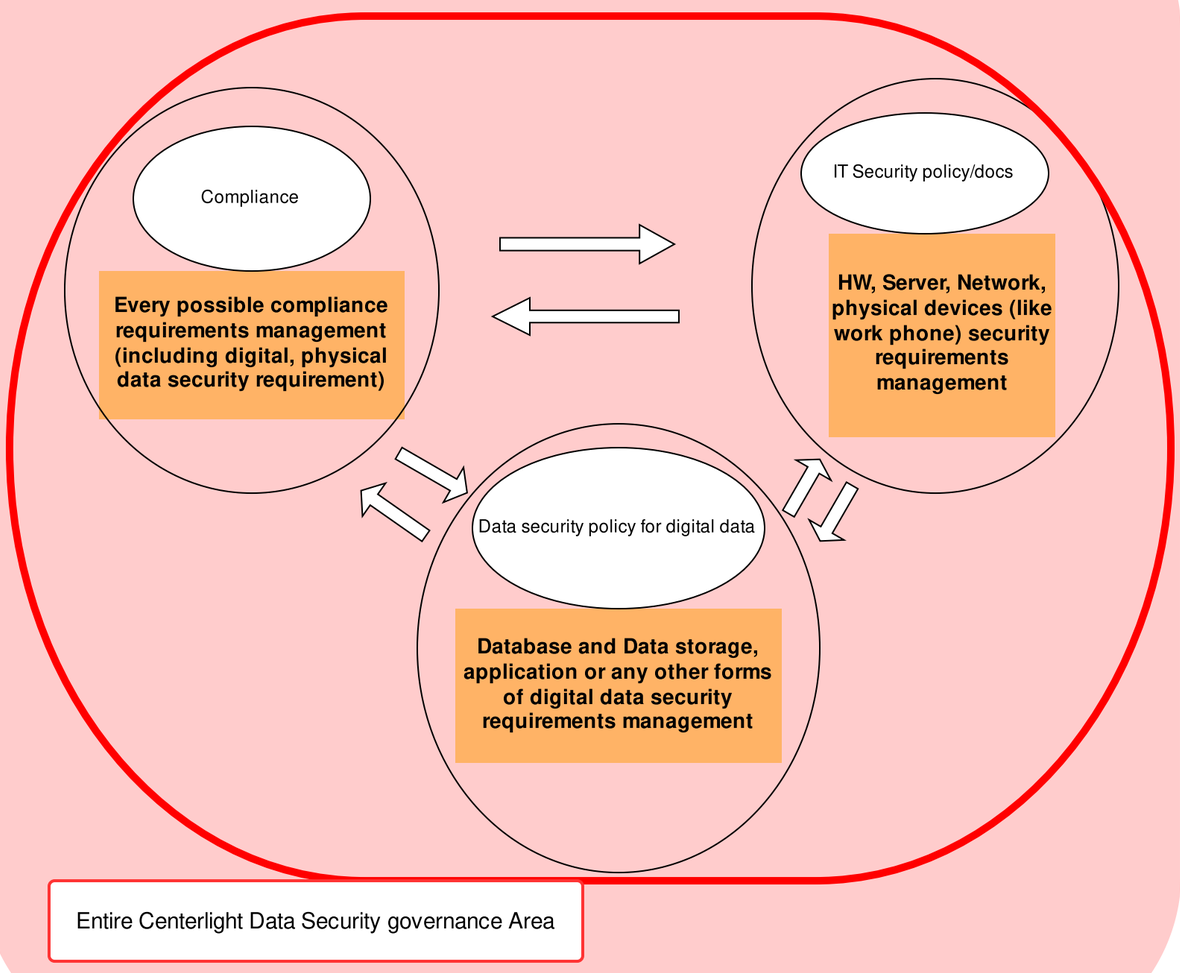
Objectives of this policy:
- Protect data from unauthorized access or misuse
- Ensure confidentiality of data
- Ensure integrity of data
- Ensure availability of data when needed
- Comply with all necessary regulatory, contractual and legal requirements

In this policy, there are below sections:
Three Entities of data security in Centerlight
Authorized users of data: Refer to what Data governance policy defines
Data usage: Refer to what Data governance policy defines
Data Access control: Refer to what Data governance policy defines
Digital Data security standard management structure, sensitive data and Reporting requirements
Responsibility
Enforcement

Sensitive data definition:
Based on HIPAA rules (45 C.F.R. 160.103 - relative government site link, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
)
, it is defined as 'protected health information (PHI)' in below.
The Privacy Rule protects all 'individually identifiable health information' held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information 'protected health information (PHI)'.
'Individually identifiable health information' is information, including demographic data, that relates to:
the individual's past, present or future physical or mental health or condition,
the provision of health care to the individual, or
the past, present, or future payment for the provision of health care to the individual

Therefore, in this policy, sensitive data means individually identifiable information and/or protected health information per above privacy law.
Any data (a set of information) collected, used, organized in Centerlight - personal demographic info that identifies individual (anonymized data is not PII) or has protected health information belong to sensitive data in this policy.
In addition, any business critical data that has been defined as critical by data governance decision maker such as some financial data also belongs to sensitive data in this policy.
Especially, digital data portion of sensitive data is the scope of this policy.

1. Three Entities of data security in Centerlight



** Three entities of Centerlight data security management have different scopes and areas, but the entire goal and purpose are the same. i.e., ensuring data security and protection in Centerlight in the entire environment.

Therefore, Each Entity's security policy contributes to and helps to strengthen the whole. Normal and routine communications are encouraged and should be formed and supported by upper management level.

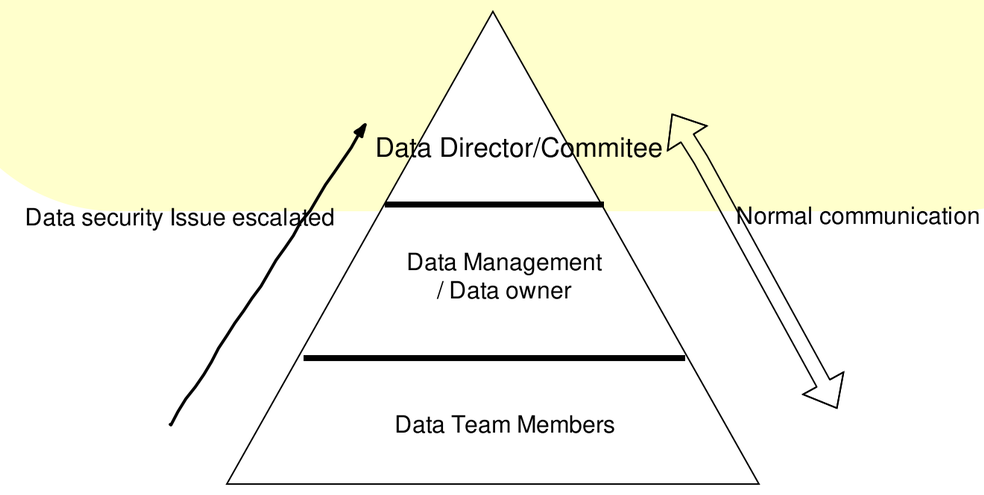
2. Digital Data security standard management structure, Sensitive Data and Reporting requirements

As defined by Data Governance policy, involved parties consist of the Director of Data, analytics, performance department, the Data Architect, a various Enterprise Database teams member/workgroups. Issues are identified and addressed by data team member (Data steward) in the first level.

In standard workflow, digital data has at least two levels: sensitive data and normal data.
Sensitive data: PII (personally identifiable information - demographic info) of CL participant or an individual that CL has a relative information, business critical/sensitive data (finance, claim, payment, tax, etc. including but not limited to being defined by finance department) and protected health information like claim, health info in sensitive data definition.
Normal data: non-sensitive data like today's date

Sensitive data primary management is defined by compliance requirements and additional input from Data Architect or Security specialist and then implemented by Data Engineering team. Technical implementation methods will be evaluated by Data Architect and Security specialist.

Issues or incidents as occur must be immediately reported to data management hierarchy (Data Architect and/or Data manger and the Director or Director committee).
On such incidents, remediation methods or procedures will be defined as a separate supplemental response procedure doc.



3. Responsibility

Digital data security is all Centerlight staff's responsibility in the end.

More specifically,
Data Architect, DBA, Data Manager are top level responsible for making and implementing security policy and any relative supplemental documentation.

Data engineer, Data Analyst, Report developer and APP engineer do normal data management works. Within work range, following guidelines/policies (especially defined by previous section 'sensitive data') are the responsibility. Also, not just following, but additional precautions and suggestions for better security environment are encouraged.

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 members' categorization in this policy. Therefore, the same responsibilities that apply to formal data team also apply.

For outside of data management/data analytics/APP team, normal Centerlight users must follow all guidelines/policies of IT security and compliance. In digital data area, if/when data access is allowed, allowed access range/permission must be observed and do protect sensitive data with all the ways per security policies.

Designated data vendors or Centerlight partners or legal auditor could get contributor permission in their own respective data area by Data governance policy states, and within the range, sensitive data protection in their boundary must be observed - example: when file with sensitive data leaves CL network area and received by vendor area, CL has no control over data at that stage. Keep the data in safe environment until the end of data life cycle is expected by Centerlight per contractual/legal agreement.

4. Enforcement

Security enforment is managed by compliance (and HR) on top view - this is general and foremost rule.

However, the first line of data security enforcement is Data Management chain and Data manager.
All statements in this data security policy are also measured and enforced by Data Management chain and Data manager.