DATA GOVERNANCE:

THE PRAGMATIC WAY

Author: Nilesh Patil

emids
experience partnership.

Table of Contents

Executive Summary

Between patient care, billing and records management, the US Healthcare ecosystem churns out enormous amounts of data. The volume of data generated is rising at an annual rate of 40%, according to the research firm IDC. This is in excess of hundreds of exabytes per year! The data includes clinical, financial and administrative data, and is of immense interest to data scientists as they explore means to derive information that can bring a difference to the most important stakeholder in the ecosystem—the patients receiving care.

Healthcare companies are investing in information technology (IT) and infrastructure to capture and use data in every aspect of healthcare delivery. The various initiatives mandated by the Federal Government continue to incite change within the healthcare industry, giving rise to the importance of using data to drive innovation in areas such as: payment models, care management, population health and resource utilization. While the change continues, one element has retained its position of prime importance—data.

To make use of the data that organizations already have, integration and interoperability are taking center stage in Healthcare IT (HIT) administration. The exchange and sharing of data is seeing early adoption and technology-backed data management tools and processes are becoming primary assets. However, there is a lurking fear that the foundations and the approach towards data management is not as robust, secure and scalable as it should be in a scenario where multiple terabytes of data are generated daily. Technology can solve many issues, but an effective and comprehensive approach to the problem that stems through the entire organization is at the heart of a secure, scalable and futuristic solution.

Creating a long-term solution is where data governance comes into play. A clear understanding of data governance principles goes a long way in ensuring that financial and personal investments made towards any data management based initiative are secure, scalable and able to withstand what may come in the future. This paper aims to provide a conceptual approach on data governance principles and practices, as well as an execution-oriented guide for the implementation of data governance within healthcare organizations.

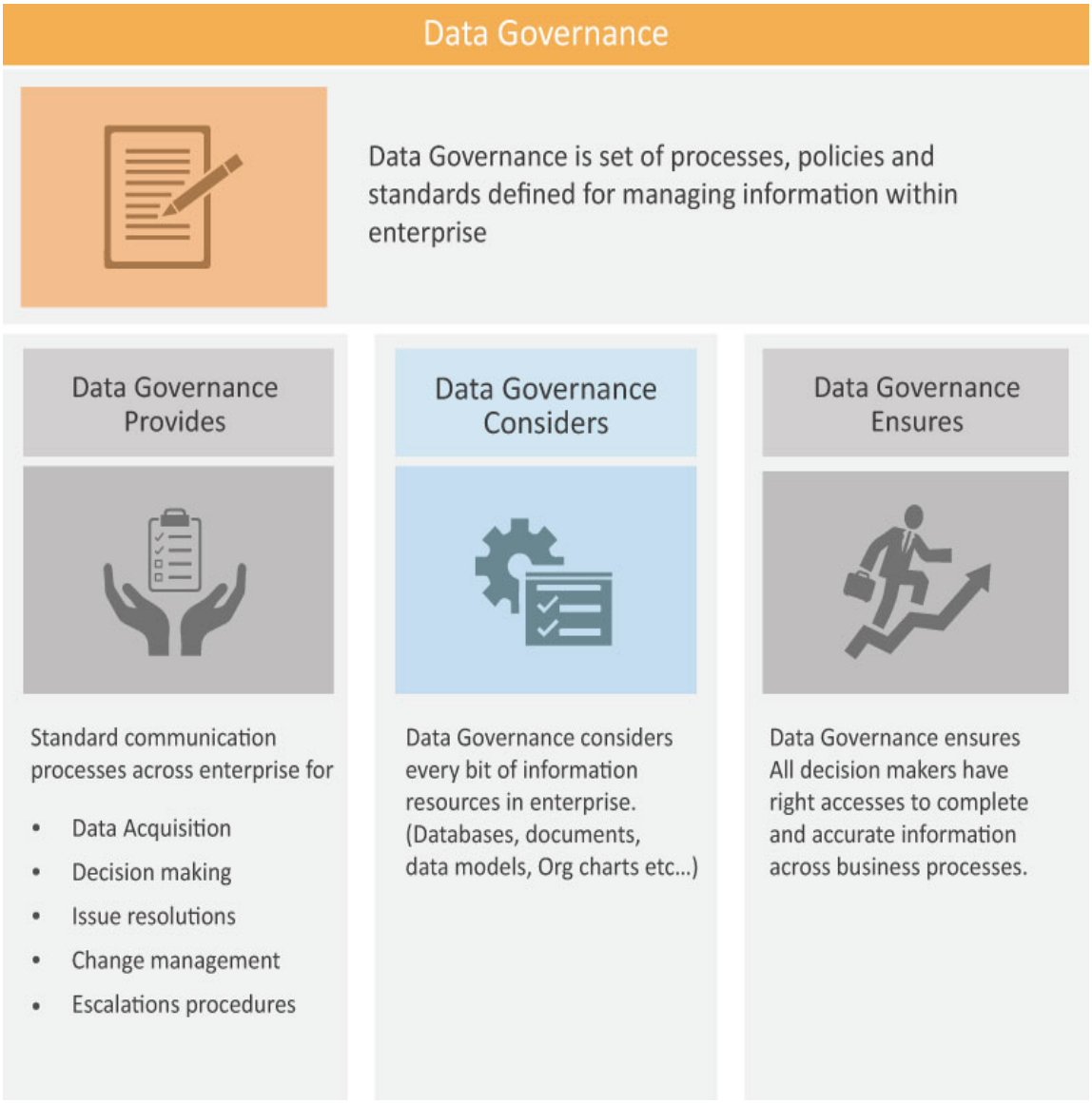
1. Background

Data volumes are more than tripling every year in the healthcare industry making data quality a big concern in many healthcare organizations. The information is under high demand, but organizing it in a way to make it consumable is a challenge many are trying to solve. Companies have a variety of database systems and platforms where the data is being stored and maintained, but are generally behind the curve on creating organization-wide solutions to manage the data. This can result in duplication of effort in data maintenance, unnecessary costs for the storage of data, as well as under-utilization of the data because it isn't formatted to solve organizational problems or provide intelligent insight for decision making. While it's often unintentional, the below chart is a cause analysis of how organizations end up with "messy data" and the risks associated:

Organizations that are victim to the segmented approach to data end up with more than the risks described above, they also have the cumbersome process of finding the right data in the right form for reporting and decision making. This often results in making decisions while only having a part of the picture. Integrating operational and analytical data for the right reports is more than an internal housekeeping issue, it's a critical issue that adds costs to the bottom line, whether from bad decision making or additional direct costs for managing the data. However you look at it, organization-wide data management is a big concern.

2. Solution

So how does an organization take control of its data and make it useful? The answer is implementation of data governance. Just like an organization would put processes and policies in place to complete projects or provide services, it needs processes and policies in place to manage the data created from these interactions. Given that the data comes from multiple functions, departments, etc., both a holistic view and organizational-wide reach are required to consider all data points, communicate requirements and ensure accessibility. Often a third party is a good option to establish this purview, as stakeholders often have an obstructed view from their independent functional area. Below is a chart that summarizes the components of proper data governance:



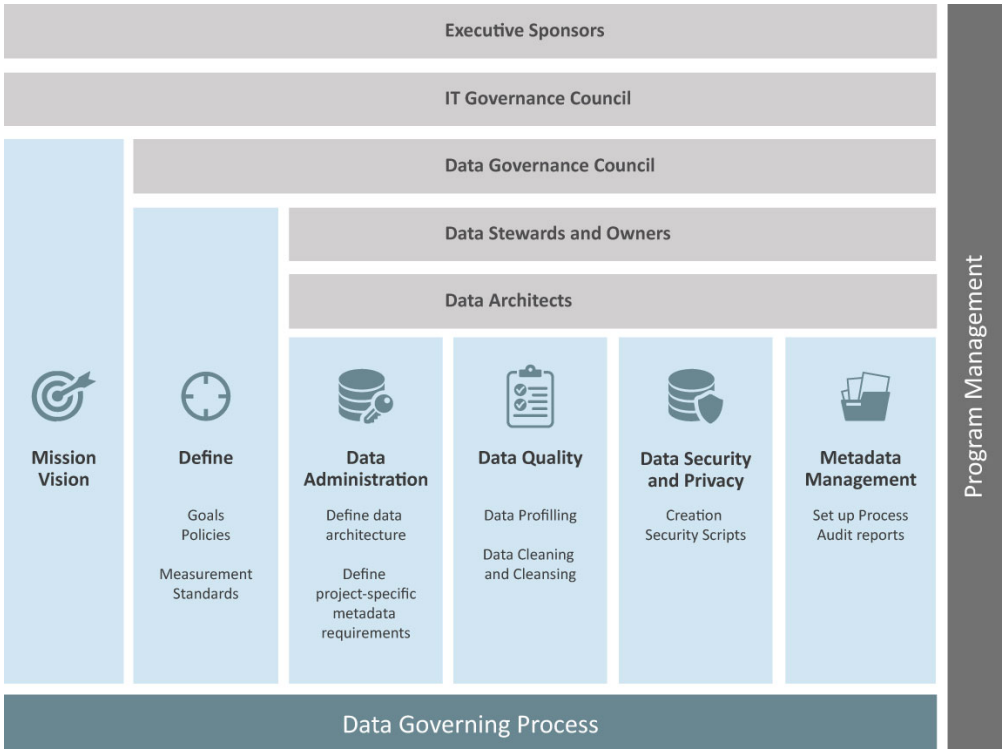
3. The Framework & Strategic Guidelines

To get started, it is important to have executive buy-in and begin with communication from the top. A Data Governance Organization (DGO), consisting of key individuals within the organization, should be created and supported by top-level leadership. A DGO must have the right mix of architects, subject matter experts, business owners and data consumers, as well as other skills that are engaged in maintaining data within the organization.

This group should have a clear charter and directive to unambiguously define the charter by explaining roles, responsibilities, processes, policies and activities required to successfully complete the data governance project. This charter, and the importance of the governance itself, should then be communicated to the entire organization.

Also note, it is also important to incentivize the DGO for the results of data governance efforts. This means a monitoring and measuring framework is essential to the success of data governance efforts. It is good practice to tie each metric to the performance review of each DGO team member.

The graphic below depicts a framework for data governance noting some of the key functional areas required and their associated responsibilities.



Though data governance has to be implemented across the entire organization, it is always good practice to start with a smaller segment. The best place to start is with implementation on the data warehouse, the master data management and the metadata management initiatives. The learnings and findings from these implementations can then be translated on a larger scale throughout the organization.

As the project commences and data is analyzed, quality will be come a key variable. A data quality strategy and framework should be considered. If implemented appropriately, it will control costs and the quality of data across the entire organization, making the value realized from the data governance implementation even greater.

In summary, below are some key considerations when determining a strategy for a data governance program.

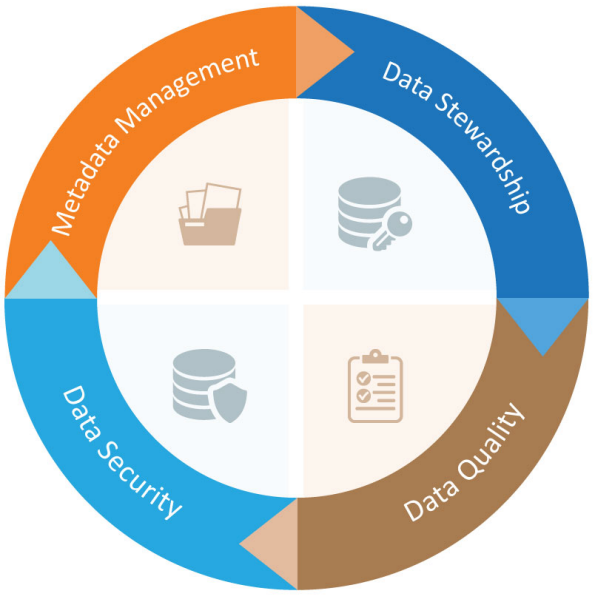
- **The right people**: Visible leadership from the executive level is very important and has to be secured before starting these efforts.
- **The right strategy**: Vision and scope must be clearly defined and derived from a thorough understanding of the current state.
- **Communication**: The strategy and objectives should be clearly outlined in a charter document and shared throughout the organization.
- **Measurement**: Selecting the right set of metrics to measure the current state and future state is very important as it will determine the success of the engagement and provide goals for those doing the work.
- **Data Quality**: Ensure quality at the source as that will affect the down stream systems consuming the data.

4. Core Components

A data governance program has four core components:

- Data Stewardship
- Data Quality
- Data Security/Privacy
- Metadata Management

Each of these components is critical to the overall program.

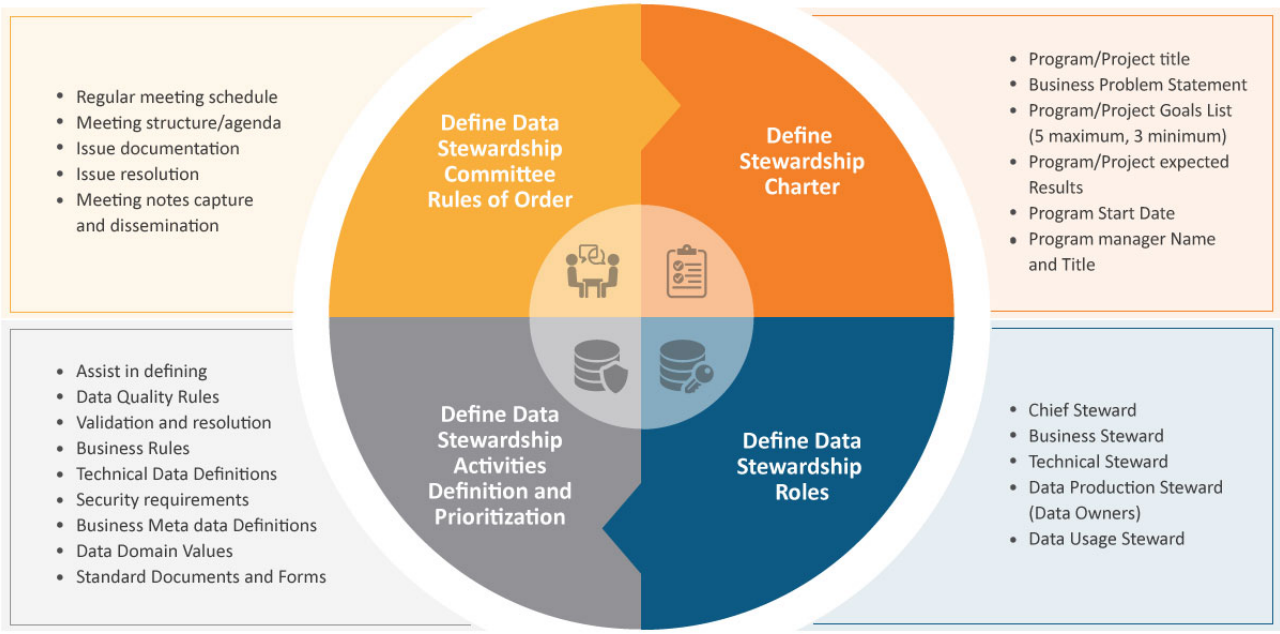


4.1 Data Stewardship

Data stewardship is perhaps the most important component of a data governance program. It supports the base for the continuance of the program beyond the initial implementation and ensures proper representation across the organization. Data stewardship is the aspect of data governance that focuses on managing data throughout its lifecycle. It provides the appropriate access to business and IT users, helping them to understand the data and take ownership of the quality and security of the data. Poor data stewardship can lead to failure of the data governance initiatives.

4.1.1 Data Stewards

A data stewardship committee integrates key players in data management and ensures cross-functional inclusion or ongoing management. The role of the data stewardship committee should be defined for the organization by creating detailed activities and standard operating procedures. The graph below depicts the requirements for forming the stewardship committee and its responsibilities:



4.1.2 Identifying Participants

Identifying the right set of people as stewards is critical to the success of data governance programs.

Logical represntation of data flow will help identify the right stewards in the organization. It is best practice to obtain an existing business user who is ingrained within the organization and current on the requirements. Placement of non-skilled, non-experienced or part-time users on the data stewardship committee should be avoided.

Key questions to answer:

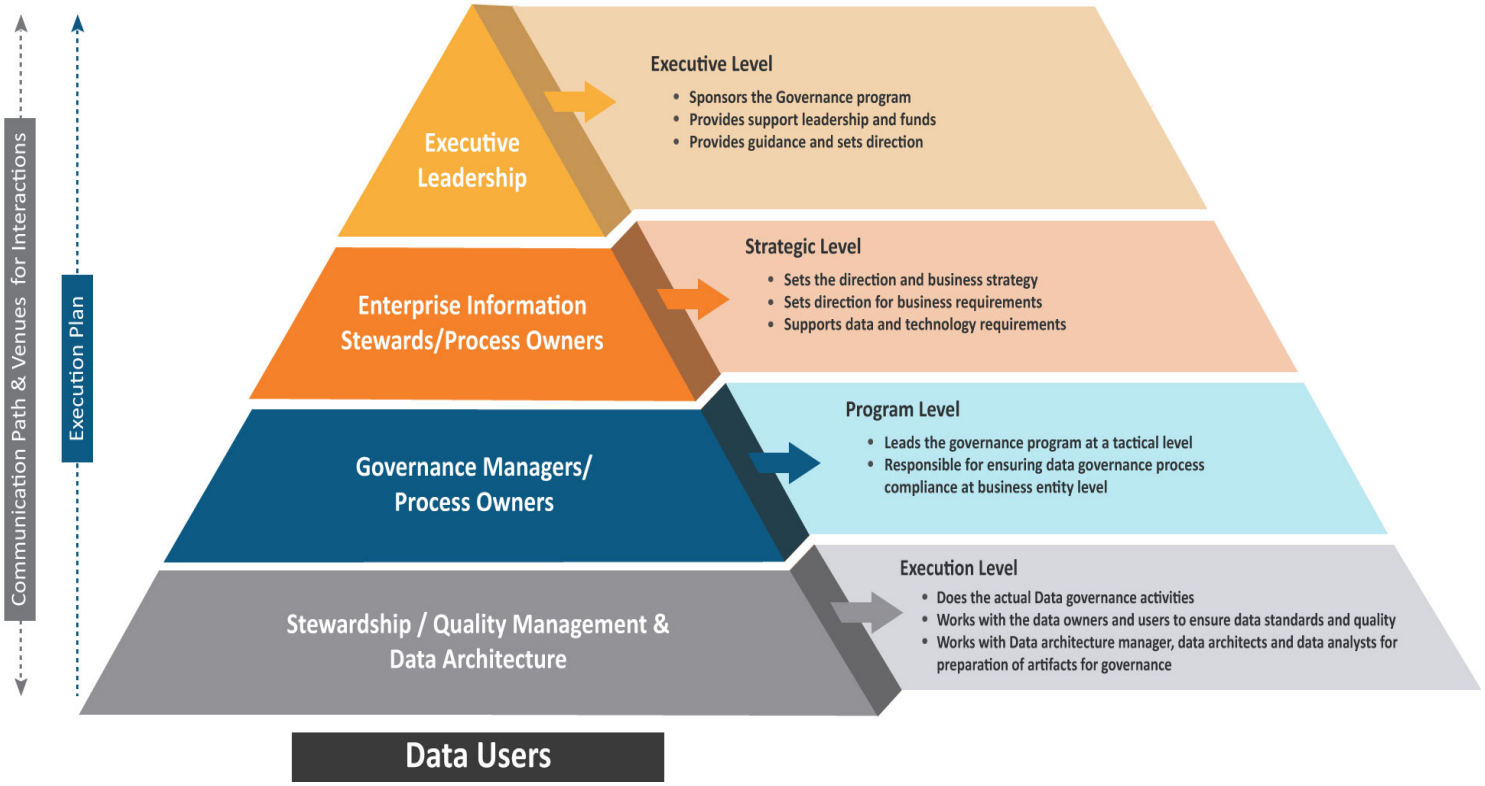
- How is the individual responsible for governing that data?
  - Does the Data owner or consumer process the data or change the data?
- What is the incentive of participating in a data governance program?
- What will be their contribution to the data governance program?
- Do participants have support from their managers?
- Do their managers appreciate and reward the data governance efforts?
- Do they have decision-making capacity in organization?

4.1.3 Governance Structure

Data governance programs fail due to a variety of reasons but the main cause is the governing structure that was put into place. As stated previously, communication and framework are critical factors to initiate a program, but people, process and technology will carry it through to completion. Creating the correct structure with no overlapping responsibilities is the point where an organization should start. If this already exists, then verifying the procedures and policies is the next step.

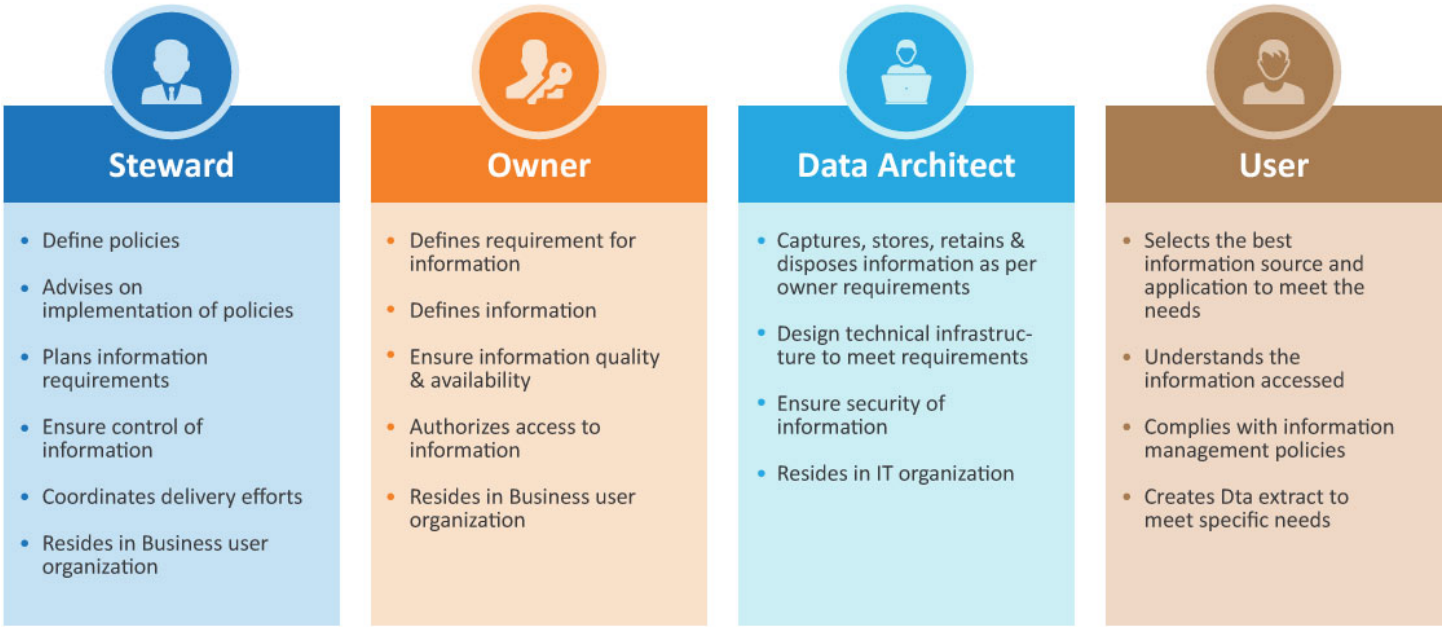
A data governance structure has multiple levels for execution. Priority should be given to developing clear procedures and policies for the four most critical levels listed below.

- *Executive* Level—responsible for providing sponsorship, i.e. funding, infrastructure and resources. This level of leadership needs to be visibly engaged for data governance programs to be successful.
- *Strategic* Level—sets the vision for data governance initiatives, providing direction and overall business strategy. Roles include enterprise-level information stewards, enterprise-level business process owners and appropriate technology representation such as enterprise data architects.
- *Program* Level—is responsible for establishing policies, procedures and standards for subject areas, business processes and technologies. As a group, this level is also responsible for maintaining the interaction and management of the governance process. Typical roles are data governance manager, data governance council, data stewards and business process owners.
- *Execution* Level—is responsible for implementing and executing data policies and procedures into business processes and various applications. Typical roles are data stewards, project team members that implement data policies, and anyone who is creating, updating or consuming the information in their day-to-day activities.



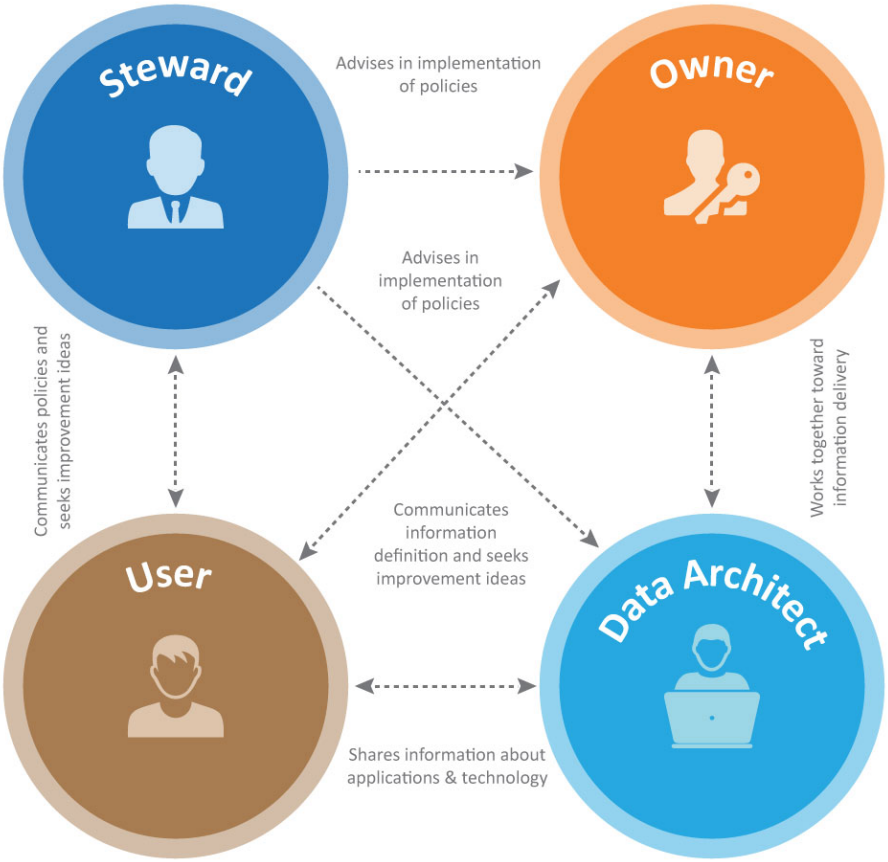
4.1.3.1 Roles and Responsibilities

Once roles are identified based on the pyramid in previous section, it is very important to define the responsibilities for each role and update the charter based on any changes within the organization or people involved. It is also important to make sure that roles are not overlapping and that each role has the necessary decision making powers for their respective areas. Examples of roles and associated responsibilities are shown below:



4.1.3.2 Communication Framework

For successful data governance program, it is very important to have a proper framework for communication. A typical communication framework is shown below:



4.2 Data Quality

Data quality is a big concern for every healthcare consumer in today's world. Poor data quality can lead to poor decision-making in both billing and care. Systems use patient data to drive transaction processing and data quality issues can cause errors. As an example, using patient data in the automated mailing of letters related to a specific condition—say, diabetes—can result in the following errors:

- Missing data might cause a patient with diabetes to be omitted and the diagnosis lost.
- Invalid duplication of a patient record might result in duplicate letters for the same person.
- Merging patient records incorrectly might cause someone without the given condition to receive a letter stating they have an inaccurate diagnosis.

Further, many payer systems today have challenges in deriving a single patient record for providers. Member identifiers in the payer systems are not always available or even correct. For example, a supplicate NPI, a missing SSN, middle name or date of birth can result in a record not matching up or worse—matching up incorrectly with another patients data. The right set of data quality rules and data quality standards are very important. It is equally important to monitor and measure the data quality and based on performance, make the necessary changes for continued improvement.

4.2.1 Define Data Quality Strategy

A clear vision and definition of data quality is what makes the program successful. In order to establish the parameters of data quality, industry benchmarks and goal setting should be a primary consideration.

The key aspects to be considered in defining the strategy for data quality are:

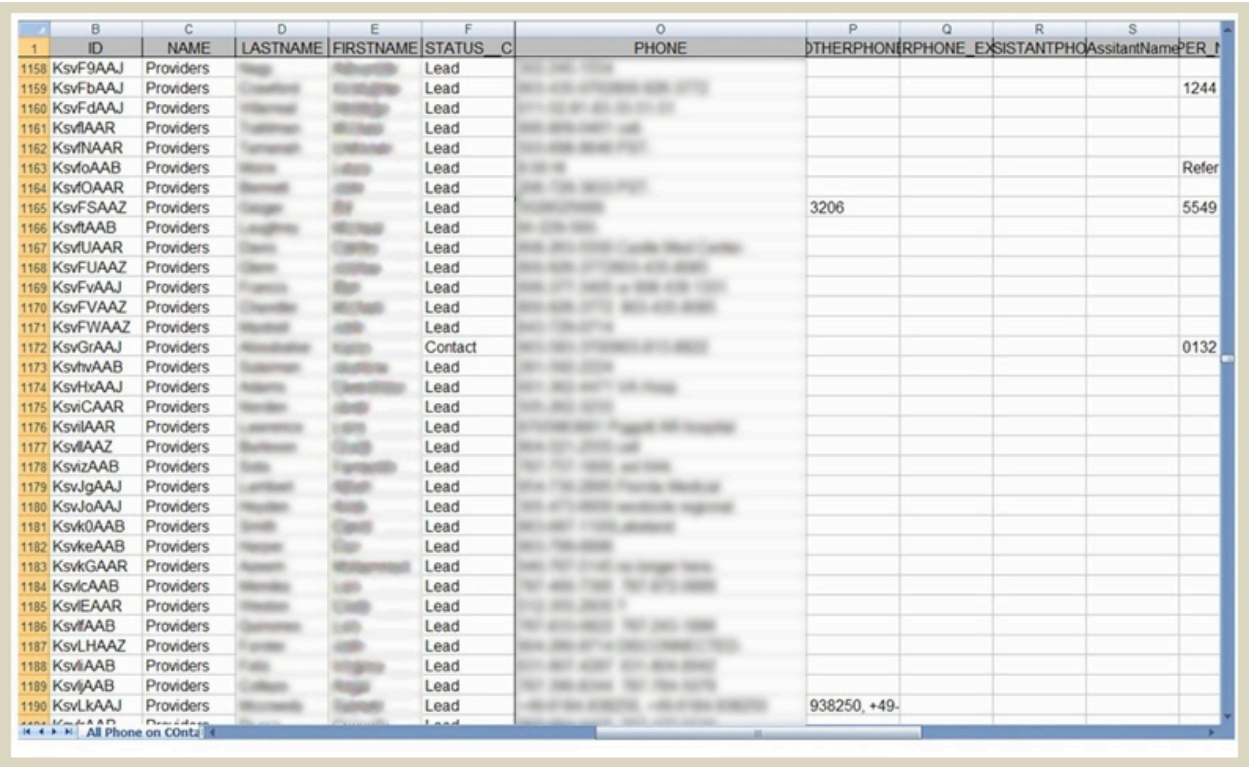
- Industry standards for available data (based on business type)
- Organizational data standards
- Level of rejection accepted
- Timelines for data availability
- Data quality metrics
- Goals for data quality metrics
- Data quality rules for specific fields and/or tables

4.2.2 Measure: Current Data Quality

In multitudes of diverse data stores and databases, it is a significant task to set and measure the level of quality. With the help of profiling, querying, reporting tools, user interviews, logs etc. the following types and traces of information can be helpful to determine data quality levels:

- Explicit column properties
    - Data type, length, range, permitted values, null, unique, patterns
- Inaccurate data values
- Inconsistent representation of same value
- Missing values
- Violation of structure rules
    - Non-unique primary keys
    - Primary key/foreign key pair orphans
    - Synonym discrepancies
- Violation of data validation rules
    - Required Fields
    - Default Values
    - Date ordering
- Violation of business data rules

Below is an example of poor data quality standards, resulting in inconsistent and inaccurate records of individual phone numbers:



	B	C	D	E	F	O	P	Q	R	S	
1	ID	NAME	LASTNAME	FIRSTNAME	STATUS__C	PHONE	OTHERPHONE	RPHONE_EX	SISTANTPHO	AssitantName	PER_I
1158	KsvF9AAJ	Providers			Lead						
1159	KsvFbAAJ	Providers			Lead						1244
1160	KsvFdAAJ	Providers			Lead						
1161	KsvfIAAR	Providers			Lead						
1162	KsvfNAAR	Providers			Lead						
1163	KsvfoAAB	Providers			Lead						Refer
1164	KsvfOAAR	Providers			Lead						
1165	KsvFSAAZ	Providers			Lead		3206				5549
1166	KsvftAAB	Providers			Lead						
1167	KsvfUAAR	Providers			Lead						
1168	KsvFUAAZ	Providers			Lead						
1169	KsvFvAAJ	Providers			Lead						
1170	KsvFVAAZ	Providers			Lead						
1171	KsvFWAAZ	Providers			Lead						
1172	KsvGrAAJ	Providers			Contact						0132
1173	KsvhvAAB	Providers			Lead						
1174	KsvHxAAJ	Providers			Lead						
1175	KsviCAAR	Providers			Lead						
1176	KsvilAAR	Providers			Lead						
1177	KsvlIAAZ	Providers			Lead						
1178	KsvizAAB	Providers			Lead						
1179	KsvJgAAJ	Providers			Lead						
1180	KsvJoAAJ	Providers			Lead						
1181	Ksvk0AAB	Providers			Lead						
1182	KsvkeAAB	Providers			Lead						
1183	KsvkGAAR	Providers			Lead						
1184	KsvlcAAB	Providers			Lead						
1185	KsvlEAAR	Providers			Lead						
1186	KsvlfAAB	Providers			Lead						
1187	KsvLHAAZ	Providers			Lead						
1188	KsvliAAB	Providers			Lead						
1189	KsvljAAB	Providers			Lead						
1190	KsvLkAAJ	Providers			Lead		938250, +49-				

Source: Google Images

4.2.3 Analyze: Data Quality

Data quality can be achieved if factors associated with the data and the data sources are well analyzed and profiled. The following considerations can make a large impact on the quality of reports and associated decision-making.

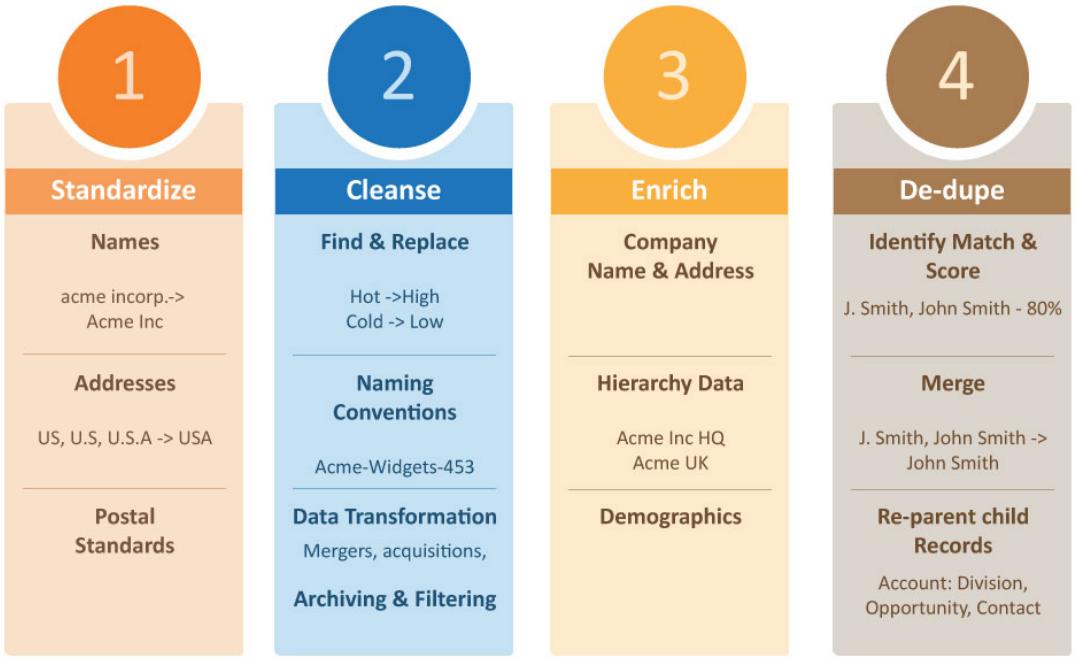
- Understand your Data Sources
  - Where is everything coming from?
  - Identify System of Record for each data element
- Understand your Data Weaknesses
  - Rate data—consider completeness, accuracy, validity, relevance, integrity, level of standardization and duplication
- Understand Mapping and Usage of Data
  - Entity Level Mapping (Provider, Member, Medical codes, Claims etc)
  - Field Level Mapping (state, city etc)
  - Duplication of information between entities
- Inspect Data Values (Visually/Tool)
  - Value/frequency list, boundary points (high/low values), (short/long values), values with special characters, random walk through data
- Structural Analysis
  - Functional dependency analysis

- Primary keys
- De-normalized sets and their sub-key
- Derived columns
- Coincidences

4.2.4 Improve: Design and Apply Data Quality Techniques

Execute your data quality plan: find it, clean it, and keep it clean.

- Standardize—i.e. Provider names, member names, addresses, postal standards, phone numbers or titles, medical codes etc.
- Cleanse—find and replace bad or missing data, implement naming conventions, transform data when merging data bases or doing large imports, and archive off irrelevant and old data
- Enrich—consider purchasing 3rd party data to add company demographics or parent child hierarchy data to your accounts
- De-dupe—define what a dupe is (or what makes a record unique) and then do an initial de-dupe, consider ongoing de-duping, or manual or automatic controls to prevent/minimize the creation of duplicates
- Validate—for any larger cleansing projects you may want to clean the data in the UAT/pre-prod and test the results before loading it back into production



Best Practices for Data Quality

- Avoid stale and bad information from spreading
  - Integrated solutions make it easier for users and more reliable for customers
  - Create links or integrated apps to avoid duplicates in many systems
  - Use and monitor 'review dates' for key objects, i.e. account plans
  - Archive or flag old/irrelevant data, i.e. contacts not updated in last "x" months
  - Use workflow and approval processes before updating key fields
- Make some information read only
  - Use processes like "case submission" to update account master information
- Train users on data quality rules, naming conventions, address conventions, dupe definitions, dupe prevention process and data importing policies

4.2.5 Control: Monitor Data Quality

Maintaining high-quality levels must be a regular practice and cannot be viewed as a one-time activity. The following parameters need to be closely monitored, using data quality dashboards, to ensure that data quality levels have not slipped.

- Number/percentage of duplicates
- Percentage of data changed
- Percentage of data cleansed
- Percentage of records rejected
- Comparison between quality last data load vs. current data load
- Percentage of missing values
- Percentage of nulls

4.3 Data Security

Securing health data is not merely a business requirement for organizations, but rather an obligation and commitment. It is important that close attention is given from all stakeholders to ensure that standard security guidelines are adopted, monitored and improved at all times. This aside, organizations are also encouraged to frame their own policies and measures beyond standard guidelines. After all, a well-rounded data security plan is part of a good data governance practice and it consequently, rolls up to sound corporate governance.

4.3.1 Define: Policy for Data Security

As a part of the data governance initiative, defining and communicating a policy for data security is essential. Organization-wide initiatives must be carried out to ensure that all employees, especially those dealing directly with data, are well versed with the policy. A comprehensive data security policy must include the following:

- Policy scope
- Data Classification—confidential vs. non confidential
- Data security policy statement
- Data security compliance (industry/organization) needs
- Breach of policy and enforcement rules
- Data life cycle
- Data security responsibilities
- Management responsibilities

4.3.2 Measure: Current Data Security

On a periodic basis, the data security measures adopted need to be assessed and measured. This will help administrators to remain aware of the actuals, be better prepared for any eventualities and take proactive measures as required. The following are a few guidelines to be considered while studying the current data security for all types of confidential health data:

- Talk to DBA's/Network Administrators to understand:
    - Current cryptographic mechanisms for data transmission and document gap findings
    - Current cryptographic mechanisms for data storage at rest and document findings
    - Disposal and Retention mechanisms
    - Access Control methods
    - Partitioning methods
- Study data access and activity reports for a specific period to ensure only authorized users can access data and generate a findings report with access violation incidences
- Understand Audit Reports/Compliance reports if any
- Study physical and logical access reports to find any security breach
- Conduct business user interviews to find out the data loss incidences in last month, quarter and year

4.3.3 Analyze: Data Security Issues

There must be a clearly defined frequency for data stewards to analyze data security status and any uncovered issues. It is important for them to perform a thorough root-cause analysis of issues identified from the activity reports. The typical analysis will cover the following areas:

- Inference attacks due to the wrong access privileges being granted to data users
- Unauthorized access due to dual security engines, i.e. built-in database security features within the operating system access control
- Human factors such as accidental and intentional errors, omissions, modifications, destruction, misuse, disclosure, sabotage, fraud, and negligence
- External threats such as trojans, malware, spyware etc.

Analysis should result in the evaluation of the effectiveness of security measures to determine whether the methods are:

  - Small, simple and straightforward
  - Carefully analyzed, tested and verified
  - Used properly and selectively so that they do not exclude legitimate accesses
  - Reasonably efficient in terms of time

4.3.4 Improve: Data Security Techniques

How effective have techniques been securing the healthcare data residing in your organization? Today, attempts at hacking and breaching secure environments have become more creative and innovative. Technology in the wrong hands is detrimental for data and IT administrators and they are expected to be conscious and aware at all times. Organizations managing sensitive health data need to invest time and effort in developing better data security measures. The following techniques and methods should be used for improving data security based on the data security gaps identified in the organization:

- Implement row level and column level security based on data classification. Common areas of classification are:
  - Public, when the data poses little risk
  - Private, when the data poses moderate risk
  - Restricted, when the data poses significant risk
- Establish improved procedures for account management
  - User Identification management
  - Establishing, activating, modifying, reviewing, disabling, and removing accounts
  - Review profiles regularly to ensure validity
- Establish improved procedures for access enforcement to include: access control lists, access control matrices, cryptography
- Implement multi-factor authentication
- Implement encryption of data if it is not existing

- Implement logging and event monitoring procedures if they do not currently exist
- Ensure disaster recovery with regular back-ups
- Identify personnel that have significant information system security roles and responsibilities during the system development life cycle and conduct security training

4.3.5 Control: Monitor Data Security

In a real-world scenario, healthcare data is mostly distributed in diverse systems across the organization and in some cases geographically separated. Also, data is moved around different systems as part of different transactions. In each of these steps, data is vulnerable to attacks, leaks and breaches of different magnitudes. It's an important practice to monitor, review and revisit data security measures. Continuous monitoring activities include:

- Configuration management and control of information system components
- Security impact analyses of changes to the system
- Ongoing assessment of security controls
- Management of an audit log and status reporting

It can be beneficial to use tools like Websense Data Security Suite for data protection, monitoring and endpoint data loss.

4.4 Metadata Management—Process of Data Governance

The data governance program must control the creation, implementation and adoption of all data standards, policies and procedures. While the governance council develops and sets the standards, policies and procedures for the data and metadata management, the data stewards, as enablers and executors of the policies and procedures, also have a pivotal role to play in the process of data governance.

The data governance committee must also be collaborative in all information systems application lifecycle activities (development, maintenance, evaluation, packaging and implementation) to coordinate and manage any impact these activities may have on the integrity of the organization's data.

With metadata management (standards, policies & procedures) under the ambit of the data governance program, an organization can ensure that policies remain consistent and changes or upgrades to policies, if any, can be coordinated and communicated throughout the organization.

4.4.1 Define: Metadata Standards

Metadata is imperative and is a widely accepted norm for working with the enormous amount of data that healthcare organizations deal with today. To ensure metadata is rendered useful, it is important to define the metadata standards for easy adoption and utilization. The following aspects need to be defined for metadata standards:

- Business Process Metadata
  - Semantic descriptions of a table's columns/business terms
  - Controlled vocabularies/data dictionaries
- Technology Metadata
  - Metadata standards for specific business
    - Naming standards for tables, files, reports etc.
    - Abbreviations (systems and business)
    - Code values
  - Metadata standards such as XMI (XML Metadata Interchange) or SGML (Standards Generalized Mark-up Language) a standard for exporting and importing metadata
  - Common Warehouse Metamodel for source and target metadata
- People Metadata
  - People activity metadata i.e. activity log
  - End user metadata to satisfy compliance reporting

4.4.2 Measure: Current Metadata Effectiveness

The effectiveness and the utility of resident and available data are affected by the approach adopted for metadata management. While the low quality of metadata can render data underutilized, superior metadata management can enhance usability. A metadata management process must tie in periodic business user interviews to assess the effectiveness of the metadata management process while analyzing the existing landscape for each type of metadata:

- Business Process Metadata
  - Inventory of existing data assets and corresponding metadata in the enterprise
- Technology Metadata
  - Identify sources of meta data (CASE tools, existing databases and files, paper documentation)
  - Identify current metadata import/export standard
  - Identify how technology meta data is used in organization
  - Recording the cycle time for getting compliance reports
- People Metadata
  - The availability of people metadata and its usability in the organization
  - Study current audit reports

4.4.3 Analyze: Metadata Effectiveness

A periodic deep-dive analysis of metadata is essential to understand the gaps that exist in data dictionaries and to formulate ways to address those gaps. A typical metadata analysis includes following:

- Business Process Metadata
    - Identify gaps in the available data dictionaries and the required metadata for all business processes and analyze reasons for those gaps. Common reasons include:
        - Metadata not captured at source
        - Metadata changed by consuming application but not documented
        - Metadata management tool not effective enough to store lineage of data
- Technical Metadata
    - Analyze gaps in the required and the available metadata for data models, database tables/entities, data sets, structures, etc. These gaps could be a result of metadata not being defined for reports, schedules, tables, etc
- People metadata
    - Identify gaps in data available and required for compliance reporting and find reasons for those gaps. A common reason for this could be that the metadata management tool is only used to capture process metadata and no other metadata in the organization.

4.4.4 Improve: Metadata Standards and Procedures

The following can be techniques and methods used for improving metadata management for people, process and technology metadata:

- Prioritize metadata required for compliance and identify metadata that can be easily accessed and stored by the metadata tool
- Implement a metadata adoption process for the long-term strategic needs of the enterprise
- Preferably include metadata for key business/technology owners
- Implement metadata integration process/routines
- Implement metadata standardization routines/procedures
- Create a deployment plan for the enterprise
- Single, authoritative source ('registration authority') for each metadata element
- Reuse metadata where possible for statistical integration as well as efficiency reasons

4.4.5 Control: Monitor Metadata Management

Metadata Management is monitored via monthly metadata reports. Some of examples include:

- Database Metadata Report:
  - What are database table, columns, keys, indexes, relationships etc.?
- Data Model Metadata Report:
  - What are the definitions of the business entities?
  - What attributes make up these entities?
  - What is the business definition of the attributes?
  - What are the allowable values for the attributes?
  - What is the relationship between the logical data model and the physical data model?
- Data Movement/Transformation Metadata Report:
  - How was the data derived? Using calculation, conditionals, both?
  - Is the value of this data depends on the values of other data? What data and how?
  - What was done when data was missing?
  - What action was taken when source data did not fall within quality guidelines?
  - When is the data moved?
- Business Rule Metadata Report:
  - What is the relationship between two entities of data in the logical data model?
  - What are the conditions under which a piece of data can take on certain values?
  - How is data created, updated, deleted?
  - When are rules established? By whom?

5. Common Pitfalls

While most enterprises agree that data governance is an important cog in the wheel, there can be different reasons for data governance not delivering the desired results. The most common failure points for data governance programs can be one or more of the following:

- Lack of accountability and strategic participation
- Lack of data standardization across organizations IT infrastructure
- Lack of awareness of business value of data
- Failure to manage data quality early in the data governance process
- Cross-divisional/cross-departmental issues
- Failure to recognize outcome specific measures (KPIs)
- Lack of compliance monitoring
- Lack of proper training and awareness of data governance policies

6. Conclusion

Healthcare enterprises are dealing with different varieties of sensitive user data and it is multiplying at an exponential rate. Data governance provides a credible degree of order, consistency and clarity for managing healthcare data. With payers increasingly exploring the value-based payment path, providers going the last mile towards population health management, technology innovations enabling patients to take control of their own health, and federal mandates driving initiatives for greater data-driven healthcare delivery, the explosion of data governance requirements will only continue. In such an imminent eventuality, a comprehensive data governance program is a necessity for stable business operations.

*At the core of **EFFECTIVE** data governance lays the **RIGHT**:*

- Stewardship and Governance Model
- Data Quality
- Data Security
- Metadata Management

*…which helps companies to be **CONFIDENT** of the **INFORMATION** that they:*

- Analyze
- Report
- Action

…so that they can be confident that their financial statements, strategic decision making, and compliance activities are:

- Complete
- Accurate
- And Timely

About the Author

Nilesh Patil – Director, Business Intelligence Practice, emids Technologies

Mr. Patil has over 13 years of experience in data management, business intelligence and establishing data management platforms and practices for enterprises. He has successfully managed and delivered various Master Data Management, Data Governance, Data Warehouse and BI projects.

7. References

Data Governance: A Necessity in an Integrated Information World

By Danette McGilvray (DM Review Magazine)

Metadata Management and Other Considerations for

Enterprise-Wide Business Intelligence Implementations

By Marianne Arents, ThinkFast Consulting

BI Strategy: What's in a Name? Data Governance Roles, Responsibilities and Results Factors

By Rich Cohen (DM Review Magazine)

Five Ms of Meta Data

By Arup Duttaroy (DM Review Magazine)

Objective of the Data Security Model

By George Barroso, Brian O'Connor & Xu Zhao (DM Review)