SUBJECT:	DATA INTEGRITY POLICY
CHAPTER:	INFORMATION MANAGEMENT
AUTHOR:	CHIEF INFORMATION OFFICER

PURPOSE:

Numerous regulations at the state and federal level require healthcare organizations to ensure the integrity of both clinical and financial information that is collected, stored, manipulated and shared with other organizations for purposes including, but not limited to: clinical performance, operations, reimbursement and compliance. This policy reflects high level requirements for data integrity. Other key information management standards may be found in policies addressing compliance with the Health Insurance Portability and Accountability Act (HIPAA) as well as the information security policy maintained by the County's Information Services Department (ISD).

POLICY:

It is the responsibility of each Department to ensure these data integrity measures are applied in all settings where data is utilized in the course of official business. This includes both paper-based information management processes as well as automated information systems.

Data integrity can be described across five domains: Completeness, Consistency, Validity, Accuracy and Availability.

1. Completeness is a measure by which all required data is included. This includes the following characteristics:
    a. Data has been included from all required/ expected sources in the population (no missing sources).
    b. All the records that should be included for each source have been included (no missing records).
    c. Individual records included are complete/ all required data fields are included (no null or blank data fields).
2. Consistency is a measure by which data adheres to a common definition for its meaning and use.
3. Validity is a measure by which data adheres to defined business rules, accepted values and accepted formats.
4. Accuracy is a measure by which data contains correct values. Accurate data not only adheres to integrity constraints and measurement rules but is data that reflects actuality.
5. Availability is a measure by which data can be accessed when required and by the appropriate people. It is current and up-to-date at the time of release / use.

PROCEDURES:

1. **Establish Data Integrity and Validation Controls:** Department Managers and Health Information Technology system owners are responsible for establishing controls that support the completeness, consistency, validity, accuracy and availability of data. A data integrity risk management methodology should be employed to address the limitations and factors that can lead to a loss in data integrity. The most common limitations include:
    a. *Coverage:* Not all appropriate data is present
    b. *Capture and collection:* Measures do not exist to minimize error or omission in data capture or data supply
    c. *Unit Non-response:* Not all records have been submitted or included
    d. *Item (Partial) Non-response:* Records received are not all complete
    e. *Measurement Error or Bias:* Problems with consistency – errors in the data collected/reported
    f. *Edit and imputation:* Data received not validated to detect and remediate incorrect or missing data
    g. *Processing and estimation:* Errors in the processing and aggregation of data received
    h. *Data Currency:* Data is not up to date at the time of release
    i. *Data comparability:* Data not consistent over time or uses inconsistent conventions
    j. *Data accessibility:* Data not readily accessible
    k. *Documentation:* Insufficient supporting documentation to interpret and utilize the data
    l. *Adaptability and relevance:* No mechanisms to adapt to developments, emerging issues for the data

    A matrix of the relationships between these factors and the five domains of data integrity is included in the Appendix as a means to assess the impact of data integrity risks.

2. **Maintain Integrity of Collected/Transmitted Data:** The Medical Center's processes and practices intended to ensure the integrity of data include the following:
    a. Comprehensive manuals, updated as required, are provided for the guidance of Medical Center staff, software vendors and users of the data
    b. Formal records are maintained of any changes to source data
    c. Permanent secure storage of the original submissions of data are maintained for auditing purposes and conform to County policy
    d. Secure transmission of data conforms to County policy, including file encryption and secure transmission over the Internet
    e. Logging of data transmission events is maintained (class of data, file/report names, sender recipient, date, etc.)
    f. Regular auditing of original submissions against final warehoused data is undertaken to ensure the integrity of the validation and transformation/derivation steps.
    g. In addition, the Medical Center undertakes regular analysis of data after validation processing, to identify outliers, inconsistencies, variance between time periods and apparent unusual patterns in output data.

3. **Inform Data Users of Their Responsibilities:** Department Managers are responsible for informing all data users of their responsibility to maintain the confidentiality and integrity of the data. Department Managers are also responsible for ensuring all data users complete mandatory information protection and compliance training. Refer to SMMC HIPAA and compliance policies for detailed responsibilities.

REFERENCES:

Data Integrity Guidelines for Health Services, Office of Data Integrity, Commission on Hospital Improvement, Melbourne, Victoria, Australia : http://health.**vic**.gov.au/chi/**data**.htm

VPS Data Integrity Manual, Department of Treasury and Finance, Melbourne, Victoria, Australia: www.dtf.vic.gov.au

San Mateo Medical Center HIPAA Policy Library:
http://intranet.co.sanmateo.ca.us/smmc/hipaa/hipaa.html

San Mateo County Information Technology Security Policy:
http://intranet/Intranet/IntranetHome/Policies%20and%20Standards/security.htm

San Mateo County Email Policy:
http://intranet/Intranet/IntranetHome/Policies%20and%20Standards/email.htm

Implementation:	09/2013
Reviewed and approved by:	Date:
Director, Information Management	9/13
Chapter Chair	9/13
Chief Information Officer	9/13
Chief Medical Information Officer	9/13
Chief Executive Officer	9/13, FINAL
	9/23/2013
Old number(s): N/A	
Received for review: (date) from (committee) or (person and dept)	
NOTE(S):	
STATUS:	

APPENDIX

Data Integrity Risk Assessment Methodology

			Data integrity impact				
			Completeness	Consistency	Validity	Accuracy	Availability
	Limitation category	**Category definition**					
1	Coverage	Not all appropriate data is present	X	X		X	
2	Capture and collection	Measures do not exist to minimize error or omission in data capture or data supply	X	X	X	X	X
3	Unit Non-response	Not all records have been submitted or included	X	X			
4	Item (Partial) Non-response	Records received are not all complete		X	X		
5	Measurement Error or Bias	Problems with consistency – errors in the data reported		X	X	X	
6	Edit and imputation	Data received not validated to detect and remediate incorrect or missing data	X	X	X	X	X
7	Processing and estimation	Errors in the processing and aggregation of data received	X	X		X	
8	Data Currency	Data is not up to date at the time of release	X	X	X	X	X
9	Data comparability	Data not consistent over time or uses inconsistent conventions	X	X	X	X	
10	Data accessibility	Data not readily accessible	X	X	X		X
11	Documentation	Insufficient supporting documentation to interpret and utilize the data		X			X
12	Adaptability and relevance	No mechanisms to adapt to developments, emerging issues for the data		X	X		X