ePHI Data and System Integrity Policy

Applies To:	All	Policy Number:	ITS-0050
Issued By:	AVP for IT	Policy Version Number:	1.0
Date Issued:	January 21, 2022	Last Review Date:	January 21, 2022
		Last Revised Date:	January 21, 2022

University of Detroit Mercy will protect ePHI from unauthorized alteration, destruction, or disclosure by implementing reasonable and appropriate measures to facilitate the maintenance of reliable system components, workflows, and data.

University of Detroit Mercy will implement processes to corroborate that ePHI has not been altered or destroyed in an unauthorized manner, as well as document current organization procedures in line with all newly implemented policies relating to data and system integrity. Determinations as to the type of mechanism(s) to utilize will be made as follows:

- **Electronic authentication.** University of Detroit Mercy will implement electronic mechanisms when they are available, employable, and commensurate with the risks associated with the ePHI

- **Procedural authentication.** If electronic authentication mechanisms are not available, or in order to augment electronic mechanisms, University of Detroit Mercy will implement procedural mechanisms when appropriate based upon the risks associated with the ePHI

Procedures, including, but not limited to, backup verification, hardware, and software reviews, to periodically check data and system functionality to identify integrity issues will be utilized by University of Detroit Mercy. These procedures will be performed at least annually.

The workforce is required to report all suspected vulnerabilities or unauthorized ePHI modification/destruction to the Security Officer. The Security Officer will report all suspicious findings that may indicate a security incident or other violation in accordance with University of Detroit Mercy's security incident reporting procedures.

Control procedures will be implemented for information system(s) development and/or changes in an effort to reduce the risk of operator or system errors that could result in incidents, including, but not limited to, unauthorized disclosures of or access to ePHI, unexpected downtime or data errors.

Notes

- Data integrity can be compromised by both technical and non-technical sources
  - Accidental/intentional changes that improperly alter or destroy ePHI
  - Electronic media errors
  - Electronic media failures

4001 W. McNichols Road
Detroit, Michigan 48221-3038
313-993-1500
www.udmercy.edu

- Identify security measures to reduce risks to the integrity of data

- Determine if existing information systems have the ability to automatically check for data integrity
  - Check sum verification
  - Digital signatures

History and Updates
January 21, 2022: Initial Policy