ISO/TR 21332:2021 (E)

Health informatics — Cloud computing considerations for the security and privacy of health information systems

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviated terms

5 Cloud computing

- 5.1 General
- 5.2 Overview of cloud computing
- 5.3 Cloud computing roles and activities
- 5.4 Cloud capabilities types and cloud service categories
- 5.5 Cloud deployment models
- 5.6 Cloud computing information system security capabilities

6 Considerations for health information in cloud computing environment

- 6.1 Overview
- 6.2 Health information security
- 6.2.1 Overview of Teleworking Policies and Procedures
- 6.2.2 Telework and portable devices
- 6.3 Information security policies
- 6.3.1 Overview
- 6.3.2 Information security and protection of PII and PHI
- 6.3.3 Availability
- 6.3.4 Cloud deployment models considerations
- 6.3.5 Audit trail and logs
- 6.3.6 Cryptography and obfuscation
- 6.3.7 Retention, backup, and deletion
- 6.3.8 Access control and multi-client segmentation
- 6.3.8.1 General
- 6.3.8.2 Assets and performance control
- 6.3.8.3 Legal and accountability
- 6.3.9 Change management
- 6.3.10 Disaster recovery
- 6.3.11 Testing and evaluation
- 6.3.12 Information management

Annex A (informative) Example guidance from the UK for selecting and risk managing cloud based digital health services

- A.1 Guidance and recommendations for selecting
- A.1.1 General
- A.1.2 Overview
- A.2 Recommendations
- A.2.1 Recommendation 1 – Understand
- A.2.2 Recommendation 2 – Assess
- A.2.2.1 General
- A.2.2.2 Risk Appetite
- A.2.2.3 Governance

A.2.2.4 Other considerations
A.2.2.4.1 General
A.2.2.4.2 Public perception
A.2.2.4.3 Lock in and migration
A.2.2.4.4 Data repatriation
A.2.2.4.5 Existing situation
A.2.2.4.6 Complex systems
A.2.2.4.7 Data residency and sovereignty
A.2.2.4.8 Fair Processing
A.2.2.5 Documentation
A.2.2.6 Contracts
A.2.3 Recommendation 3 – Implement
A.2.3.1 General
A.2.3.2 Select a cloud provider
A.2.3.3 Apply security controls
A.2.3.4 Documentation
A.2.4 Recommendation 4 – Monitor
A.2.4.1 General
A.2.4.2 Manage known risk
A.2.4.3 Monitor cloud service
A.2.4.4 Monitor controls

Annex B (informative) Detailed advice and guidance

Annex C (informative) Service classification recommendations

Page count: 54