

ISO/TR 15801:2017-05 (E)

Document management - Electronically stored information - Recommendations for trustworthiness and reliability

Contents		Page
Foreword		vi
Introduction		vii
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Information management policy	2
4.1	General	2
4.2	Information management policy document	2
4.2.1	2
4.2.2	ESI covered	3
4.2.3	ESI roles and responsibilities	3
4.2.4	ESI security classification	3
4.2.5	Storage media	4
4.2.6	Data file formats and compression	4
4.2.7	Outsourcing	4
4.2.8	Standards related to information management	4
4.2.9	Retention and disposal schedules	5
4.2.10	Information management responsibilities	5
4.2.11	Compliance with policy	5
5	Duty of care	5
5.1	General	5
5.1.1	Trusted system	5
5.1.2	Controls	5
5.1.3	Segregation of roles	6
5.2	Information security management	6
5.2.1	Information security policy	6
5.2.2	Risk assessment	7
5.2.3	Information security framework	8
5.3	Business continuity planning	8
5.4	Consultations	8
6	Procedures and processes	9
6.1	General	9
6.2	Procedures manual	9
6.2.1	Documentation	9
6.2.2	Content	9
6.2.3	Compliance with procedures	10
6.2.4	Updating and reviews	10
6.3	ESI capture	10
6.3.1	General	10
6.3.2	Creation and importing	11
6.3.3	Information loss	11
6.3.4	Metadata	12
6.4	Document image capture	12
6.4.1	General	12

6.4.2	Preparation of paper documents	12
6.4.3	Document batching	13
6.4.4	Photocopying	13
6.4.5	Scanning processes	14
6.4.6	Quality control	15
6.4.7	Rescanning	17
6.4.8	Image processing	17
6.5	Data capture	17
6.5.1	Data creation	17
6.5.2	Conversion and migration	18
6.6	Database considerations	18
6.6.1	General	18
6.6.2	Database systems	18
6.6.3	Database schemas	20
6.6.4	Master data management	20
6.6.5	Transactional vs. updating	21
6.7	Indexing	21
6.7.1	General	21
6.7.2	Manual indexing	21
6.7.3	Automatic indexing	21
6.7.4	Index storage	21
6.7.5	Index amendments	22
6.7.6	Index accuracy	22
6.8	Authenticated output procedures	22
6.9	ESI transmission	23
6.9.1	Intra-system ESI transfer	23
6.9.2	External transmission of files	23
6.10	Information retention	24
6.11	Information preservation	25
6.12	Information destruction	25
6.13	Backup and system recovery	25
6.14	System maintenance	26
6.14.1	General	26
6.14.2	Scanning systems	26
6.15	Security and protection	27
6.15.1	Security procedures	27
6.15.2	Encryption keys	27
6.16	Use of contracted services	28
6.16.1	General	28
6.16.2	Procedural considerations	28
6.16.3	Transportation of paper documents	29
6.16.4	Use of trusted third party	29
6.17	Workflow	29
6.18	Date and time stamps	30
6.19	Version control	30
6.19.1	Information	30
6.19.2	Documentation	30
6.19.3	Procedures and processes	31
6.20	Maintenance of documentation	31
7	Enabling technologies	31
7.1	General	31
7.2	System description manual	32
7.3	Storage media and sub-system considerations	32
7.4	Access levels	33
7.5	System integrity checks	33
7.5.1	General	33
7.5.2	Digital and electronic signatures (including biometric signatures)	34
7.6	Image processing	34
7.7	Compression techniques	35
7.8	Form overlays and form removal	36

7.9	Environmental considerations	36
7.10	Migration	36
7.11	Information deletion and/or expungement	37
8	Audit trails	37
8.1	General	37
8.1.1	Audit trail data	37
8.1.2	Creation	38
8.1.3	Date and time	38
8.1.4	Storage	38
8.1.5	Access	39
8.1.6	Security and protection	39
8.2	System	39
8.2.1	General	39
8.2.2	Audit trail information	40
8.2.3	Migration and conversion	40
8.3	ESI	40
8.3.1	General	40
8.3.2	ESI capture	40
8.3.3	Batch information	41
8.3.4	Indexing	42
8.3.5	Change control	42
8.3.6	Digital signatures	42
8.3.7	Destruction of information	43
8.3.8	Workflow	43
	Bibliography	44