IT Security, Change Management, and Resilience Overview

IT security deals with the protection of information technology and protection of maintenance of data confidentiality, integrity, availability, and accountability. In review of the resilience management the organization must describe how the organization manages business continuity in the event of total or partial system outages, both planned and unplanned. A coordinated communication process to inform impacted staff of the scope and expected duration of the outage will be reviewed. It will be necessary to have a clear communication plan when it is necessary to move to use downtime documentation.

The inspectors should be enabled to understand:

- Management of Business Continuity
- Availability of clinical data during an outage
- Mechanism to ensure downtime PC is operational
- Demonstration of standard operating procedures for downtime
- Statistic about regular staff training

ID	Stage	Y	N	Compliance Statement
33	3			**Role Based Access Control** Role Based Access Control (appropriate access to information systems is based on staff role).
34	5			**BC policy w/ Root Cause Analysis** Business Continuity policy contains Root Cause Analysis templates and lessons learned reports.
35	6			**BYOD policy; annually review** Bring your own device policy is agreed, implemented and reviewed every 12 months.
36	6			**BC plan understood by staff; annually training** Staff understand the Business Continuity plan and participate in, at a minimum, a disaster drill that simulates an enterprise wide outage of all systems every 12 months.
37	6			**Information assets managed across the enterprise** Information assets (network devices, software, interfaces, etc.) are proactively managed across the enterprise. An assessment is performed annually to identify risks to the infrastructure. The risk assessment and any issues identified by monitoring are escalated.
38	6			**Process to effectively communicate system changes** There is a process to effectively communicate system changes, based on impact and relevance, to all users. (Training if required is automatically scheduled and registries updated.)
39	6			**New devices and SW changes are risk assessed and authorized** To maintain patient safety the IT Change Management process ensures that all new devices and software modifications are risk assessed and authorized for use by the clinical safety officer.
40	6			**Scheduled and unscheduled outages are standardized** Outages are standardized for both scheduled and unscheduled disruptions in information systems. Disruptions are defined (e.g., planned, unplanned), reported, and tracked by organizational leaders. A mature process is in place defining time interval before paper and recovery sequence.
41	6			**Downtime PC w/ encrypted patient data** Patient data is encrypted on the downtime PC and password protected.
42	6			**During downtime: Summary reports ensure patient data integrity** Patient Data integrity is maintained during downtime using summary reports including patient allergies, medication profile, patient problem/diagnosis, department schedules, other.

Navigation: Table of Content – Summary

ID	Stage	Y	N	Compliance Statement
43	6			**Downtime PC on the ward w/ printer connection** Summary reports are available on a device on the wards / floors when the system is down – PC/workstations on a generator circuit or UPS and direct connected to a printer on a generator circuit or UPS.
44	6			**Staff awareness of downtime processes** Staff demonstrate awareness of downtime processes and available IT resources during downtimes. The organization evaluates the impact of downtime on staff and clinician teams.
45	6			**Clinical data integrity management during / after system outage** The organization manages clinical data integrity during and following a system outage by backloading clinical data into the EMR and the disposition of any clinically relevant paper.
46	6			**Simulated Disaster Recovery events are conducted** Simulated Disaster Recovery events are conducted, and lessons learned are implemented into protocols to manage downtime.
47	7			**Frequency of unscheduled outages are measured annually** Frequency of unscheduled outages are measured annually (i.e., has been measured over the past 12 months). An outage is determined when a clinician must resort to using paper to document care. That paper must then be scanned into the EMR and any orders backloaded.
48	7			**Long-term downtime processes** Demonstrated long-term downtime processes describe what the organization does in the event of a downtime, informed by documented guidelines for extended downtimes.
49	7			**Simulated Disaster events incl. downtime ClinDoc and recovery** The organization performs a simulated disaster event annually. The simulation must include downtime clinical documentation and recovery of data created during the downtime. This simulation does not affect the production environment.
50	7			**Communication plan for downtime procedures** A communication plan clearly outlines when to, or not to implement downtime procedures.
51	7			**Service interruptions are measured** Service interruptions that cause the creation of downtime documentation are measured by the number of downtime documents scanned into the EMR.