# Statement of Applicability (SoA) of MedSecure Hospitals Pvt. Ltd

| Control | Annex A Control | Applicability | Justification | Document Reference | Status |
|---|---|---|---|---|---|
| 5.14 | Information transfer | Yes | Applicable because staff share patients reports through unauthorised platforms (eg. WhatsApp) which could impact the confidentiality.(R003)<br>Introducing, maintaining and regularly updating a secure data transfer platform for sensitive data to ensure confidentiality. | Risk Register: R003 | Not Implemented |
| 5.16 | Identity Management | Yes | Applicable because ex-employees may retain access to the system which could lead to unauthorised access (R005).<br>Implement identity management control to manage the lifecycle of the users account. | Risk Register: R005 | Implemented |
| 5.19 | Information Security in Supplier Relationships | Yes | Applicable because third party laboratories upload patients reports directly to the hospital system which may lead to unauthorised access of the data risking confidentiality, integrity and availability of the sensitive data.(R009)<br>Implementing information security in supplier relationship control shall establish an appropriate method of sharing the sensitive data. | Risk Register: R009 | Not Implemented |
| 5.20 | Addressing Information Security within Supplier Agreements | Yes | Applicable because there is no agreement between the hospital and the third party laboratories upon sensitivity of the patients reports that shall compromise the confidentiality, integrity and availability of the report when uploaded directly in the hospital system. (R009)<br>Establish an agreement where the laboratories and hospital ensure to maintain the confidentiality, integrity and availability of the data. | Risk Register: R009 | Partially Implemented |
| 5.21 | Managing Information Security in the ICT Supply Chain | Yes | Applicable because changes in supplier services (e.g., new third-party laboratory software or upgraded data-sharing platforms) may introduce new vulnerabilities if not assessed for information security impact (R009). Managing these changes ensures that confidentiality, integrity, and availability of patient data remain protected. | Risk Register: R009 | Not Implemented |
| 5.22 | Monitoring, Review, and Change Management in Supplier Services | Yes | Applicable because supplier services (e.g., third-party laboratories) require continuous monitoring and periodic review to ensure they maintain agreed security controls. Without monitoring, changes or lapses may go unnoticed, risking unauthorized access (R009) | Risk Register: R009 | Not Implemented |
| 5.23 | Information Security for Use of Cloud Services | Yes | Applicable because sensitive patient records are shared between third-party laboratories and the hospital. Without secure cloud-based controls (e.g., encryption, access restrictions), data could be exposed to unauthorized access (R003, R009). | Risk Register: R003, 009 | Not Implemented |
| 6.13 | Information Security Awareness, Education, and Training | Yes | Applicable because doctors are unaware of the information security of the sensitive data and their neglegence can risk the confidentality, integrity and availbility of the data. (R010)<br>Scehdule training & awareness program and document the record of the program to avoid regulatory non-compliance. | Risk Register: R010 | Implemented |
| 5.30 | ICT Readiness for Business Continuity | Yes | Applicable because of the disruption the hospital's services went offline for 2 days and the data was lost during the downtime. (R007)<br>Draft, plan and implement Business Continuity Plan to avoid going off the grid. | Risk Register: R007 | Not Implemented |
| 7.1 | Physical Security Perimeter | Yes | Applicable because IT server room is unguarded that could lead unauthorized access in the room and to the sensitive data which compromises the confidentiality of the data leading to regulatory noncompliance. (R001)<br>Define the perimeter of the IT Server room and guard the area with security devices (like CCTV) for information security compliance. | Risk Register: R001 | Implemented |
| 7.2 | Physical Entry Controls | Yes | Applicable because IT server room is unguarded that could lead unauthorized access in the room and to the sensitive data which compromises the confidentiality of the data leading to regulatory noncompliance. (R001)<br>Implementing access controls (like card access, security guard) to the IT server room shall avoid unauthorized access. | Risk Register: R001 | Implemented |
| 7.4 | Physical Security Monitoring | Yes | Applicable because IT sever room will not be monitored for the unauthorized physical access, tampering, or environmental hazards.(R001)<br>Implement continuous monitoring of the secured perimeter for total information security of the server room. | Risk Register: R001 | Implemented |
| 8.14 | Redundancy of Information Processing Facilities | Yes | Applicable because data was not backed up during the 2 days downtime and it lead to disruption in the hospital's services.(R007)<br>Implement redundancy facilities and define the Recovery Point Objective (RPO) & Recovery Time Objective (RTO) to reduce the downtime. | Risk Register: R008 | Not Implemented |