**Policy Compliance Checklist**

**Purpose**

To evaluate and ensure consistent adherence to clinic security policies.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Policy Area** | **Compliance Criteria** |  | **Compliant? (Yes/No)** | **Responsible Party** | **Review Frequency** |
| Acceptable Use Policy | Are all users aware of what constitutes acceptable/unacceptable use? |  |  | Practice Manager | Quarterly |
|  | Are personal use restrictions communicated and followed? |  |  |  |  |
|  | Are USB device approvals tracked? |  |  | IT Consultant / Manager |  |
| Access Control Policy | Are user accounts reviewed quarterly? |  |  | Practice Manager | Quarterly |
|  | Is MFA enabled for all systems? |  |  | IT Consultant |  |
|  | Are shared accounts disabled? |  |  |  |  |
| Data Protection and Privacy Policy | Are physical records locked when not in use? |  |  | All Staff | Monthly |
|  | Is data encryption in place? |  |  | IT Consultant |  |
|  | Has privacy training been completed this year? |  |  | HR/Practice Manager | Annually |
| Incident Response Policy | Are incidents reported and logged consistently? |  |  | All Staff | Ongoing |
|  | Was the last incident review documented? |  |  | Clinic Director | After each incident |
| Backup and Recovery Policy | Are daily and weekly backups occurring on schedule? |  |  | IT Consultant | Weekly |
|  | Has the last backup restore test been conducted successfully? |  |  | IT Consultant | Quarterly |