ODYSSEY SOLUTIONS OPERATOR TOOLKIT

Dental Practice IT Downtime Plan

An Odyssey Solutions planning template for safe operations during system, network, power, cloud, imaging, and cybersecurity outages.

Prepared for	[Practice or organization name]
Prepared by	Odyssey Solutions | Houston IT, cybersecurity, and HIPAA guidance

Start here: Customize every bracketed field, assign an accountable owner, and test the finished process with the people who will use it. Keep completed copies in a controlled location.

Important: This template is educational and does not provide legal, insurance, privacy, compliance, or clinical advice. It does not guarantee HIPAA compliance, insurance eligibility, security, or recovery. Confirm requirements with qualified professionals and never enter patient information, passwords, or other sensitive data into an uncontrolled copy.

How to use this plan

1. Assign names, backups, contact methods, and decision authority.
2. Complete procedures for each clinical and business workflow using the systems actually in use.
3. Keep controlled paper or offline materials where staff can reach them during an outage.
4. Exercise the plan at least annually and after major technology or workflow changes.
5. Document lessons, corrective actions, owners, due dates, and retest evidence.

Plan control record

Field	Practice entry
Organization and locations	[Practice name and covered sites]
Plan owner	[Name and role]
Approved by	[Executive or governing role]
Effective date	[YYYY-MM-DD]
Next exercise date	[YYYY-MM-DD]
Controlled copies	[Locations of paper/offline copies]
Related plans	[Emergency operations, incident response, backup, communications]

1. Activation and decision authority

Activate this plan when an outage prevents safe or reliable use of a critical workflow, affects more than [number] users or [number] locations, is expected to last longer than [duration], or may involve a security or privacy incident.

Role	Primary	Backup	Authority or responsibility	Contact method
Incident lead	[Name]	[Name]	Activates plan and coordinates decisions	[Phone / alternate]
Clinical lead	[Name]	[Name]	Patient-care and safety decisions	[Phone / alternate]
Operations lead	[Name]	[Name]	Staffing, scheduling, patient communication	[Phone / alternate]
IT lead	[Name]	[Name]	Technical triage, containment, vendors, recovery	[Phone / alternate]
Privacy/security lead	[Name]	[Name]	Evidence, privacy, legal and insurance escalation	[Phone / alternate]

2. Critical contact directory

Provider or contact	Service	Normal contact	After-hours contact	Account or contract reference
Odyssey Solutions	IT coordination and support	(832) 805-8467	[Contracted path]	[Agreement or ticket details]

Provider or contact	Service	Normal contact	After-hours contact	Account or contract reference
[Internet provider]	Internet / circuit	[Phone / portal]	[Phone]	[Account]
[Practice software vendor]	Practice management	[Phone / portal]	[Phone]	[Customer ID]
[Imaging vendor]	Imaging / sensors	[Phone / portal]	[Phone]	[Customer ID]
[Cloud / Microsoft 365]	Identity / email / files	[Admin portal]	[Escalation]	[Tenant]
[Cyber insurer]	Incident response	[Broker / hotline]	[Hotline]	[Policy]
[Legal / privacy counsel]	Legal and notification guidance	[Phone]	[Phone]	[Engagement]
[Electrical / facilities]	Power / building systems	[Phone]	[Phone]	[Reference]

3. Workflow priorities and tolerances

Workflow	System dependency	Maximum tolerable downtime	Offline method	Recovery owner
Patient identification and check-in	[Systems]	[Duration]	[Paper / alternate]	[Role]
Scheduling and confirmations	[Systems]	[Duration]	[Paper / alternate]	[Role]
Charting and clinical documentation	[Systems]	[Duration]	[Paper / alternate]	[Role]
Imaging capture and retrieval	[Systems]	[Duration]	[Alternate method]	[Role]
Prescriptions and clinical communications	[Systems]	[Duration]	[Approved alternate]	[Role]
Payments, claims, and eligibility	[Systems]	[Duration]	[Paper / deferred]	[Role]
Phones, email, and patient messaging	[Systems]	[Duration]	[Alternate routing]	[Role]

4. First 15 minutes

Done	Action
[ ]	Protect patient safety and stop any workflow that cannot be completed reliably.
[ ]	Record the time, affected users, locations, systems, symptoms, and recent changes.
[ ]	Check power, network, internet, server, cloud-service, and vendor status without making uncontrolled changes.
[ ]	Notify the incident lead and IT contact through an available channel.
[ ]	If malicious activity is possible, preserve evidence and follow the ransomware/security decision gate.
[ ]	Tell staff which approved downtime procedures to use and where controlled forms are stored.
[ ]	Set the next update time and identify who communicates with patients, vendors, and leadership.

5. Workflow downtime procedures

Scheduling and check-in

Planning prompt	Practice procedure
How will staff view the day's schedule if the practice system is unavailable?	[Document the approved procedure, owner, materials, and reconciliation step]
How will identity, consent, medical history, and arrival status be recorded?	[Document the approved procedure, owner, materials, and reconciliation step]
How will paper or offline records be reconciled after recovery?	[Document the approved procedure, owner, materials, and reconciliation step]

Clinical charting and treatment

Planning prompt	Practice procedure
Which procedures can continue safely and which must pause?	[Document the approved procedure, owner, materials, and reconciliation step]
Where are approved downtime forms and who controls completed copies?	[Document the approved procedure, owner, materials, and reconciliation step]
How will allergies, medications, treatment notes, and signatures be captured and later entered?	[Document the approved procedure, owner, materials, and reconciliation step]

Imaging and sensors

Planning prompt	Practice procedure
Can images be captured locally, and how will they be associated with the correct patient after recovery?	[Document the approved procedure, owner, materials, and reconciliation step]
Which devices, acquisition computers, bridges, and vendor services are dependencies?	[Document the approved procedure, owner, materials, and reconciliation step]
Who verifies image availability and patient association before normal work resumes?	[Document the approved procedure, owner, materials, and reconciliation step]

Phones, email, and patient messaging

Planning prompt	Practice procedure
What alternate number, device, or routing method is approved?	[Document the approved procedure, owner, materials, and reconciliation step]
Who posts service updates and what information must never be disclosed?	[Document the approved procedure, owner, materials, and reconciliation step]
How will incoming messages be recorded and reconciled?	[Document the approved procedure, owner, materials, and reconciliation step]

Billing, payments, and claims

Planning prompt	Practice procedure
Which transactions may be deferred and which approved manual processes are available?	[Document the approved procedure, owner, materials, and reconciliation step]
How are receipts, authorizations, batch totals, and payment information protected?	[Document the approved procedure, owner, materials, and reconciliation step]
Who reconciles duplicate, missing, or delayed transactions after recovery?	[Document the approved procedure, owner, materials, and reconciliation step]

6. Ransomware and security decision gate

Do not improvise: If files are encrypted, ransom notes appear, accounts behave unexpectedly, or malicious activity is suspected, do not reconnect devices, delete logs, contact an attacker, or restore systems until the incident lead and authorized responders decide the next step.

Done	Action
[ ]	Disconnect affected devices from networks only when authorized and safe to do so.
[ ]	Preserve screenshots, alerts, timestamps, logs, messages, and affected-device details.
[ ]	Contact Odyssey or the contracted IT/security responder through a trusted channel.
[ ]	Notify the cyber insurer and legal/privacy contacts according to the policy and response plan.
[ ]	Use a known-clean communication channel if email or identity systems may be compromised.
[ ]	Record every containment, reset, restoration, and notification decision.

7. Recovery priorities and validation

Priority	System or service	Recovery target	Prerequisite	Validation owner	Evidence location
1	[Identity / network / server]	[RTO]	[Dependency]	[Role]	[Location]
2	[Practice management]	[RTO]	[Dependency]	[Role]	[Location]
3	[Imaging]	[RTO]	[Dependency]	[Role]	[Location]
4	[Communications]	[RTO]	[Dependency]	[Role]	[Location]
5	[Billing / reporting]	[RTO]	[Dependency]	[Role]	[Location]

Done	Action
[ ]	Confirm identities, permissions, multifactor authentication, and administrative access.
[ ]	Verify system time, network segmentation, endpoint protection, patching, and monitoring.
[ ]	Open representative patient records without changing source data unnecessarily.
[ ]	Validate new entries, imaging links, integrations, printing, scanning, phones, email, and backups.
[ ]	Reconcile paper or offline records using a documented owner and second-person check.

Done	Action
[ ]	Monitor for recurring errors, unexpected sign-ins, missing data, or failed synchronization.
[ ]	Record who approved return to normal operations and the evidence reviewed.

8. Exercise and after-action record

Exercise date	Scenario	Locations / teams	Result	Owner	Evidence
[YYYY-MM-DD]	[Scenario]	[Scope]	[Pass / gaps found]	[Name]	[Location]

Finding or improvement	Risk / impact	Action owner	Due date	Retest date	Status
[Finding]	[Impact]	[Name]	[YYYY-MM-DD]	[YYYY-MM-DD]	[Open]

9. Distribution and maintenance

- Keep controlled copies available during power, internet, server, identity, and cloud outages.
- Review contacts at least quarterly and test critical numbers or portals.
- Review the full plan after exercises, incidents, office moves, system conversions, vendor changes, and major staffing changes.
- Destroy superseded paper copies securely and retain plan history according to policy.

Test the plan before the outage

Odyssey Solutions can map technology dependencies, validate backup and recovery evidence, coordinate vendors, run a tabletop exercise, and turn findings into a prioritized remediation plan.

Book an Odyssey consultation

Official references

- **HHS HIPAA contingency planning guidance:** https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- **HHS Security Risk Assessment Tool:** https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
- **CISA StopRansomware Guide:** https://www.cisa.gov/stopransomware/ransomware-guide
- **NIST Cybersecurity Framework 2.0:** https://www.nist.gov/cyberframework

Important: This template is educational and does not provide legal, insurance, privacy, compliance, or clinical advice. It does not guarantee HIPAA compliance, insurance eligibility, security, or recovery. Confirm requirements with qualified professionals and never enter patient information, passwords, or other sensitive data into an uncontrolled copy.