Volume 3 • Issue 2 • 2021

Review Article

Journal of Biotechnology and Immunology

Standard Operating Procedures for Business Continuity and Disaster Management in healthcare organizations

Mohamed Refaat[1]*, Marwan ElBagoury[2] and Amy Hutchinson[3]

[1]Gentium Healthcare, Cairo, Egypt

[2]University of South Wales, School of Law, Accounting and Finance, Pontypridd, Wales

[3]McMaster University, Hamilton, Canada

***Corresponding Author:** Mohamed Refaat, Gentium Healthcare, Cairo, Egypt.

Received: July 02, 2021; **Published:** September 25, 2021

Abstract [1]

Organizations are responsible for minimizing disruptions to critical business operations in the event of an incident or disaster. Business Continuity Plans (BCPs) outline a range of disaster scenarios and the steps that should be taken to recover from these scenarios and return to regular operations.

They act as a set of contingencies that minimize potential harm to operations during adverse scenarios [1]. Healthcare-providing/provisioning organizations in particular, can greatly affect their clients if service is disrupted, as medication or equipment manufacturing may halt, adversely affecting those they serve.

For this reason, it is important that all healthcare organizations create, maintain, and carry out a Business Continuity Plan to ensure the continuation of their services. Examples of scenarios that should be covered in a Business Continuity Plan include emergencies, technical failures, and staff changes or absences. This paper outlines best practice business continuity measures for the most common scenarios healthcare organizations encounter.

Key words: *SOPs. Business Continuity; Disaster Management; Healthcare organizations*

Abbreviations

Business Continuity Plan: A business continuity plan (BCP) is a plan that outlines how business processes will continue during a staff change, emergency, or disaster. Such staff changes, emergencies, or disasters might include cases where business cannot be carried out under normal conditions [2].

Confidentiality: Ensuring that information is accessible only to those with authorization and is protected throughout its lifecycle. Confidential information may be marked as such or deemed confidential by its nature, e.g. it is information that is not available in the public domain [3].

PHI: Personal Health Information.

Public Domain: “common knowledge,” i.e. information that can be accessed by the general public [4].

Consent: Voluntary agreement to an act, practice, or purpose, relies upon knowledge of the matter agreed to and voluntary agreement [5].

Citation: Mohamed Refaat, Marwan ElBagoury and Amy Hutchinson. (2021). Standard Operating Procedures for Business Continuity and Disaster Management in healthcare organizations. *Journal of Biotechnology and Immunology* 3(2).

Organizational/Institutional Information: Includes publicly available and some confidential information about organizations [6].

Personal Information: Information or opinion about an individual, may include information such as names, addresses, bank account details, clinician assessments, and health conditions [7].

Patient Information: Any information about health status, provision of health care, or payment for health care that is created or collected by a service provider and can be linked to a specific individual. The privacy and confidentiality of the patient must be respected at all times [8].

Recovery Timescale: Time infrastructure needs to be back online after a disaster. This defines the maximum downtime a company can handle and maintain business continuity.

Introduction

The Introduction should impart the relevant information and objectives to support the importance of the research carried out.

Procedures

The following procedures identify main vulnerabilities and mitigation steps designed to minimize their impacts on essential functions that must continue/resume rapidly if a disruption occurs [9]. These are the main vulnerabilities most organizations encounter, and it should be noted that a full Business Continuity Plan should be catered to the individual needs of the organization.

Results

Damage to Physical Files (Recovery Timescale = 24 Hours)

The Organization is responsible for ensuring that the redundancy and accountability of its data backup procedure leaves no opportunity for data loss [14]. The following procedures allow for this to be carried out. Several steps can be taken to protect an organization in the event of physical file damage;

1. All documents related to Patient Support Programs (PSPs) will be continually scanned and digitized [10].
2. Digitized documents and information will be backed up on a daily basis, with both paper and digital versions stored at a different location than the primary source, providing recovery capability from a disaster that may cause loss of the primary data location, such as a natural disaster or electrical outage [10]. Every backup is recorded and reported to the manager to ensure backup occurs [10]
3. Any paper-based documents are put in a Water and Fire resistant safe on a regular, continuous, basis. It is the responsibility of the related manager or Quality Assurance manager to supervise this process and provide access to the safe [13].
4. All PSP and POP related documents will be retained for 5 years in order to provide a recent physical backup in the event of losing current files.
5. No offsite storage of any marketing Authorization holder documents is allowed without written approval from the marketing Authorization holder. If requested by the client or marketing Authorization holder, the backup will be on a server not an external hard drive, to comply with security and data privacy concerns.

Database Failure (Recovery Timescale = 1 - 24 Hours) [11]

Electronic file databases should be saved and recovered using the following steps;

1. Databases should be automatically saved (Auto-Save) every 1 minute.
2. IT support will handle all software problems on a continuous basis to prevent a back log of issues that could result in a large-scale error.
3. In case of damaged Hard Disk Drive; the daily offsite backup (outlined above) is used to retrieve data for a new hard disk drive.

Electrical Outage (Recovery Timescale = 1 minute)

1. All organizations should maintain an Emergency Power Supply that will protect the organization during an electrical outage. In such an event the system must automatically move into Emergency Power Supply.
2. The Emergency Power Supply must be sufficient enough to keep the main computer and communications running for an extended period of time in order to prevent loss of data and organizational functions [12].

Loss of Communications via Fax (Recovery Timescale = 1 minute)

Email and Fax are used on a regular basis to report Adverse Events (AE)

1. In case of loss of communication via Fax; email can be used [13].

Handover and Transfer of Responsibility between Staff Members

Handover procedures are designed to ensure the continuity, consistency, and efficiency of all operations. In the event of a planned or sudden temporary or permanent absence, business must continue smoothly. This is accomplished via the take-over of a named successor or back-up employee (see APPENDIX 1 and 2) [14].

The type of handover depends on the length and circumstance of the absence, knowledge of the backup person, and the nature of the responsibilities/duties being handed over.

The process of handover can be supported by [15] good information storage and comprehensive communication [16]. In case of employee change, handover, or integration of new team member, a transition plan is developed by the employee's manager or the Quality Assurance manager in coordination with the marketing Authorization holder (MAH) team.

This transition plan should contain [17]:

1. An official and up-to-date summary of each employee's role and designated tasks [18].
2. A list of current project-based responsibilities and contact information of the involved stakeholders.
3. A brief of the employee's current project objectives, work flow, KPIs, history, and milestones.
4. Any specific, necessary trainings required for the role.
5. These will be supervised by the employee's manager and done in coordination with the marketing Authorization holder team.
6. Handover of all documents and materials owned by the employee. (Employee's should be encouraged to keep such materials well organized and clearly labeled in order to prevent confusion during handover.)

It is the responsibility of the Quality Assurance or employees' manager to ensure staff continuously record all relevant information in a file that clarifies objectives, key performance indicators history, milestones, roles, and responsibilities of their tasks per project, and how it relates to the project's mission that can be used in the event of an absence [19].

In the event of a planned absence, it is the responsibility of the outgoing person to prepare a handover file under the supervision of their manager. This file should contain the most up-to-date task documentation for a smooth transition. It is the responsibility of the employee's manager or the Quality Assurance manager to ensure this process is completed [20].

In the event of a sudden employee absence or departure, it is the responsibility of the outgoing employee's manager or the Quality Assurance Manager to ensure handover files and related process are completed. Their responsibilities also include training the backup person and documenting the process [21].

Discussion

Train Backup [22]

It is the responsibility of the outgoing employee's manager or the Quality Assurance manager to ensure the preparation, training, and readiness of any employee acting as a back-up person in compliance with the governing Standard Operating Procedures and project tasks before they begin work.

For planned long-term or permanent absences there should be an overlap of duties (where possible). Ideally with the back-up person performing a work shadow of their predecessor to gain a better understanding of the role.

If such an overlap is not possible, an existing staff member could serve as a bridge. For a short-term absence, the back-up person should be briefed before the person goes on leave to allow time for follow up questions.

Retrain Predecessor

When the staff member returns from their absence, it is the responsibility of the backup to prepare a handover file that provides updates on the status of tasks.

This should be done under the supervision of the acting manager or Quality Assurance Manager who will then record and store these files for future references [16,23].

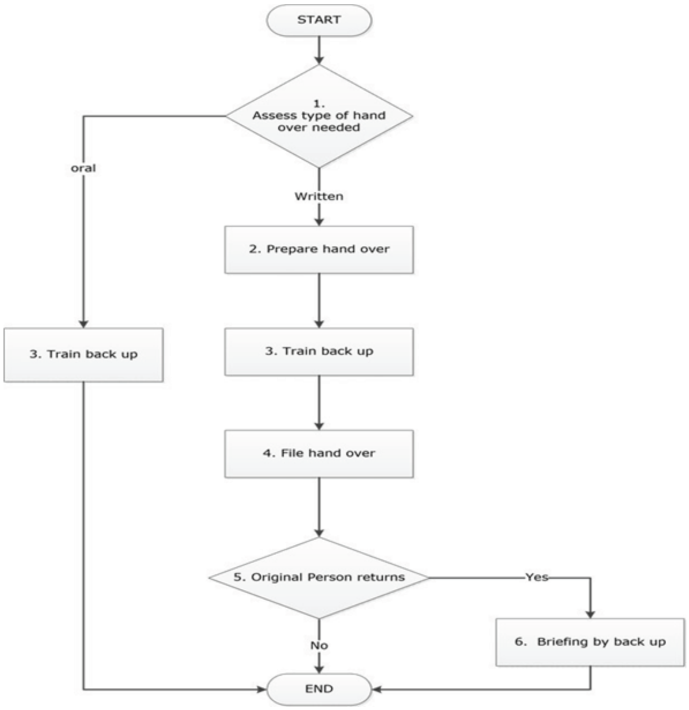
Testing the Business Continuity Plan (BCP) [24]

The following types of exercises can be used on a quarterly basis to test the BCP. This not only identifies gaps in the outlines procedures but also helps maintain employee preparedness and awareness.

1. Staff orientation meeting
2. Tabletop exercise
3. Offsite information access test

Conclusion

APPENDIX 1 (Process map/ flow chart for handover and responsibility transfer) [25]



Onboarding Report Form [26]

To be used by Direct Manager/Operations Head and other staff. Documentation should be retained as a record of completion by direct manager and QA manager.

Name of new employee:	
Start Date:	

Pre- Arrival:

Action	Manager's Notes
Inform team of new employee's appointment and start date; ensure name is added to staff lists	
Identify and order equipment (desk, chair, pc, stationery, email address, 'phone number)	
Appoint an old employee to support the new employee during induction; the old employee should be assigned before the new employee's start date, and should be briefed on their responsibilities	
Send welcome letter advising the new employee of joining instructions (venue, time, contact, documentation); contract of employment	
Provide optional information that could be useful for helping the new start prepare for their new position (Organization chart, strategy documents, job description, etc.,)	
Assigning the employee on the needed onboarding and mandatory training and keep the training logs	
Actions completed upon arrival / Handover Documentations: Date: Manager's signature:	

Task Handover Template [17]

Project Name	
Departing Associate Name & Job Title	
Backup/Bridge Associate Name	
Associate's Manager	
Start Date of Handling Process	

Handling Process	Comments
Job/Task Description	
Trainings specific to Job/Task in concern and training documentations	
Job/Task relevant Documentations, Materials and forms	
Job/Task relevant program task orders	
Access tools (Credentials, passwords, keys)	
A list of Job/Task and program responsibilities	
A list of involved stakeholders with their contacts.	
On boarding on the project's objectives, flow,	
KPIs, history and milestones	
Employee's Manager Dated Signature	
Backup/Bridge person Dated Signature	

Citation: Mohamed Refaat, Marwan ElBagoury and Amy Hutchinson. (2021). Standard Operating Procedures for Business Continuity and Disaster Management in healthcare organizations. *Journal of Biotechnology and Immunology* 3(2).

References

1. Jorrigala, V. Business Continuity and Disaster Recovery Plan for Information Security; (2017).
2. What Is BCDR? Business Continuity and Disaster Recovery Guide https://searchdisasterrecovery.techtarget.com/definition/Business-Continuity-and-Disaster-Recovery-BCDR (accessed May 15, 2020).
3. Privacy Policy - APMHA https://apmha.com.au/privacy-policy/ (accessed May 11, 2020).
4. RTW Rehab Privacy and Confidentiality Policy 1 PRIVACY AND CONFIDENTIALITY POLICY.
5. Privacy Policy | Fighting Chance https://fightingchance.org.au/privacy/ (accessed May 11, 2020).
6. Code of Federal Regulations: LSA, list of CFR sections affected - Google Books https://books.google.com.sa/books?id=V0yGAAAAMAAJ&pg=PA708&lpg=PA708&dq=Organizational/institutional+information+includes+publicly+available+and+some+confidential+information+about+organizations.&source=bl&ots=fXhQU3-ITf&sig=ACfU3U23tl2VZn06UbsE0Wt7WXNDcEtekQ&hl=en&sa=X&ved=2ahUKEwiyuZOKlqvpAhUHxoUKHcirCjgQ6AEwCXoECAkQAQ#v=onepage&q=Organizational%2Finstitutional information includes publicly available and some confidential information about organizations.&f=false (accessed May 11, 2020).
7. What is personal information? — OAIC https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/ (accessed May 11, 2020).
8. Confidentiality and Privacy of Personal Data - Health Data in the Information Age - NCBI Bookshelf https://www.ncbi.nlm.nih.gov/books/NBK236546/ (accessed May 11, 2020).
9. Emergency Management Agency, F. Continuity Guidance Circular - February 2018; 2018.
10. 10. Workshop on Patient Support and Market Research Programmes.
11. What is the best way to back up data? | Computing | The Guardian https://www.theguardian.com/technology/askjack/2014/aug/28/the-best-way-to-back-up-data (accessed May 15, 2020).
12. Back-up Power - an overview | ScienceDirect Topics https://www.sciencedirect.com/topics/engineering/back-up-power (accessed May 15, 2020).
13. Gliklich, R. E.; Dreyer, N. A.; Leavy, M. B. Adverse Event Detection, Processing, and Reporting. 2014.
14. Standard Operating Procedure; (2013).
15. Clinical Guidelines (Nursing) : Nursing clinical handover https://www.rch.org.au/rchcpg/hospital_clinical_guideline_index/Nursing_clinical_handover/ (accessed May 15, 2020).
16. Handover Policy & Procedure — Win Thein & Sons Co., Ltd https://www.winthein-sons.com/handover-policy-procedure (accessed May 15, 2020).
17. The Importance of Handovers for Exiting Employees - GO1 https://www.go1.com/blog/post-importance-handovers-exiting-employees (accessed May 15, 2020).
18. Safe Handover : Safe Patients Guidance on Clinical Handover for Clinicians and Managers; 1968.
19. Neely, A.; Richards, H.; Mills, J.; Platts, K.; Bourne, M. Designing Performance Measures: A Structured Approach. International Journal of Operations and Production Management. 1997, pp 1131–1152.
20. University of Glasgow Law Postgraduate Conference (2018).
21. How to help leavers handle the handover process - The People HR Blog People HR Blog https://www.peoplehr.com/blog/2018/09/05/how-to-help-leavers-handle-the-handover-process/ (accessed May 15, 2020).
22. What is a Standard Operating Procedure (SOP) and How to Write It https://tallyfy.com/standard-operating-procedure-sop/ (accessed May 11, 2020).
23. Records Management Policy.
24. Jungmeister, A. Business Continuity Management. (2009).
25. Transfer and handover of Patients Procedure and Guidance.pdf https://www.whatdotheyknow.com/request/283674/response/706779/attach/html/8/Transfer and handover of Patients Procedure and Guidance.pdf.html (accessed May 15, 2020).
26. San Mateo County | Managers Onboarding Guide 1 Managers/Supervisors Guide for On Boarding New Employees San Mateo County | Managers Onboarding Guide 2.

Citation: Mohamed Refaat, Marwan ElBagoury and Amy Hutchinson. (2021). Standard Operating Procedures for Business Continuity and Disaster Management in healthcare organizations. *Journal of Biotechnology and Immunology* 3(2).