Data Storage, Recovery and Backup Checklists for Public Health Laboratories

DECEMBER 2018

APHL ASSOCIATION OF PUBLIC HEALTH LABORATORIES®

Introduction

Data play a critical role in the operation of a laboratory information management system (LIMS) and therefore it must be protected. Backing up files can protect against accidental loss of data, database corruption, hardware failures and even natural disasters.

Each facility must employ backup procedures to protect the data stored on the database from damage and loss. In the case of user error, media failure or catastrophic events, the system should be able to recover the information up to or near the point before failure occurred.

This document provides guidelines to laboratory managers on how to craft and implement a detailed data backup and recovery plan and carry out regular backups of data and applications. These standard operating procedures (SOPs) are in line with the best practices for database backups and restoration in case of a disaster.

Types of Backups

The following are the major types of backups which can be carried out in Microsoft SQL Server to safeguard data in case of a disaster.

- A **full backup** creates a complete backup of the database as well as part of the transaction log, so the database can be recovered when needed. This makes it easy to restore the database because all contents are in a single file.
- A **differential backup** contains all the changes which have occurred since the last full database backup. Even though this type of backup saves on storage space, a full backup must be available in order to restore the database.
- A **transaction log backup** allows for a point-in-time restore of the database because it contains all log records that have not been included in the last backup.
- **Replication** is a set of technologies for copying and distributing data and database objects from one database to another and then synchronizing between databases to maintain consistency. Using replication, data can be distributed to different locations in real time and provide the most recent snap shot of the database. It can be done as a stand-alone process or as part of an existing backup protocol. If the original database goes offline, then the application can be redirected to the second database with minimal loss of data and downtime.

Roles and Responsibilities

The roles which various stakeholders will play to ensure that backups are running and available for restoration are important to establish before an incident occurs. As the database backup is expected to be automated, the laboratory managers or the local IT teams will be responsible for copying the backups to an external media for safe storage onsite.

- **Laboratory managers/local IT personnel** ensure that the database backup has run successfully and copy it to an external hard drive.
- **LIS support team** monitors the backups remotely to ensure they are running and are copied to external storage. The team will also monitor replication at sites where it has been configured.

Backup Timing

Ideally, the backup should be automated and configured to run at night so as not affect the database and application performance during the backup. If the backup cannot be automated, then it has to be run manually every day after 4pm. The backup will then need to be copied to an external storage device and stored separately after each successful run.

In case of an automated backup failure, it should be initiated manually the following morning and the backup should be copied to an external hard drive after successful completion.

Audit and Validation

It is important to verify the database backups to ensure that recovery is possible after a disaster has occurred. Verifying a backup ensures the backup is intact physically and that all the files are readable restorable. Checking the integrity of the database is another way to validate that the backup contains all data.

Storage & Recovery Checklist

Policy

Item	Yes	No	Comment
There are policies in place for off-site storage			
There are policies in place that define record retention			
SOPs and procedures are communicated, understood and implemented by all staff as related to their responsibilities			
Up-to-date master list that comprehensively details all laboratory documents, policies and procedures is readily accessible in hard copy or electronic form			
Document control system to ensure that records and all copies of policies/procedures are:			
• Current			
• Read by personnel			
• Authorized by proper authorities			
• Reviewed annually			
• Immediately prior versions filed separately as per national policy			
There are policies in place for archiving, storing and purging records			

Infrastructure

Item	Yes	No	Comment
All LIMS system files and installation folders are accessible by all lab computers so that updates, maintenance, and restores can occur on a system-wide basis			
Records (data?) are archived so that final reports are retrievable			
The laboratory has systems specifically assigned for disaster recovery, different from the laboratory's test system which are tested regularly (e.g. every 24 hours, nightly)			
The laboratory's test system routinely (daily or weekly) pulls samples for testing and quality assurance, according to the laboratory's specified protocol			
A sample (paper copy) is flagged for testing in the recovery system and pulled from the production system. That sample is followed through the pre-analytical, analytical, and post-analytical stages to make sure its data is intact.			
All components that integrate with LIMS are backed up regularly			

The laboratory is able to preserve instrument data and reprocess them when the system is restored following a network or system failure.			
• Only authorized users have access to this data			
• All users store this data in the same medium			
• This data is kept in an archived format for QA and troubleshooting			
The laboratory has backed up data that are:			
• Accessible			
• Can be restored			
The laboratory's LIMS is available 24/7, 365 days/year (with the exception of scheduled downtime).			

Security

Item	Yes	No	Comment
There is on-site security in place to prevent physical access to the data server			
Whenever practicable, all equipment under the control of the laboratory and requiring calibration shall be labelled, coded or otherwise identified to indicate the status of calibration, including the date when last calibrated and the date or expiration criteria when recalibration is due. This equipment is stored securely and accessible only to authorized personnel. *(As stated in ISO 17025: 5.5.8: Equipment)*			
All archived results (paper or data storage methods) are properly labeled and stored in a secure location accessible only to authorized personnel			
Information access is granted and restricted in accordance with the access control policy e.g. through secure log-on, password management, control over privileged utilities, download management and restrictions, and restricted access to program source code. *(As stated in ISO 27001 9.4: System and application access control)*			
Laboratory personnel can only access the LIMS and laboratory network with assigned usernames and passwords.			
Password protocol is defined by the laboratory and understood by personnel. Protocol includes:			
• The frequency with which users must change their passwords (ideally, every three months)			
• Password criteria specifications (number of characters/numbers/special characters required)			
Passwords are unique to each individual and not shared as a practice throughout the laboratory.			

There is a designated administrator for passwords, whose roles include assigning to new employees, and resetting passwords for personnel as needed.			

Resources

Item	Yes	No	Comment
Human:			
• There is dedicated and fully functional IT support available during business hours			
• There are documented descriptions of the roles and responsibilities of the laboratory manager, LIMS manager or IT personnel (when applicable), quality manager, and others responsible for ensuring compliance			
o Role descriptions and appropriate points of contact for any problems that arise have been communicated to all laboratory staff			
Financial:			
• The laboratory has a sustainable operational budgeting strategy that anticipates the short and long- term service/maintenance needs of its systems and services. (Short-term needs include electricity, water, daily maintenance. Long term needs might include servers, networks, cabling, LIMS maintenance, updates, and procurement).			

Protocol

Item	Yes	No	Comment
The laboratory tests its disaster recovery plan on a regular basis			
If laboratory operations are down, there is a plan in place for testing to occur in another facility			

Backup Checklist

Policy

Item	Yes	No	Comment
The laboratory has procedures to protect and backup records stored electronically and to prevent unauthorized access to or amendment of these records. (As stated in ISO 17025 4.13.1.4: Control of records)			
There are documented policies and procedures for the laboratory defining:			
• Which roles in the laboratory are responsible for backup			
• • What technology is used to conduct backups			
• • How frequently backups must be conducted			
There are policies in place for ensuring back up of all components that integrate with LIMS			
There are policies in place for testing the backup restore			
Backups are tested in a test environment to make sure they restore correctly			

Backup Software

Item	Yes	No	Comment
Free to use software			
Commercial software			

Type of Backup

Item	Yes	No	Comment
Full			
• The laboratory creates a complete backup as the database as well as the transaction log			
Differential			
• The laboratory creates a backup of only the changes which have occurred since the last full database backup.			
Replication			
• If replication is configured, it is monitored daily to ensure that data is being replicated to the backup servers			

Backup Management

Item	Yes	No	Comment
Backups are automated and configured to run at night			
• If the backup cannot be automated, then it is run manually after 4 pm daily			
Monitor backups are set up using appropriate tools so the specified admin gets email or other alert for failed backups			
Obsolete backups are deleted for better performance			

Backups are validated and verified without requiring total restores each time			
Any backups saved to a hard drive are archived to a more robust media (e.g., tapes)			
Database backups are compressed and encrypted with a password to protect the data			
• The encryption is defined in the backup script.			
Backups are tested monthly to verify full data restore.			
• If backups pass integrity and recoverability tests, then they are stored and kept separately onsite and offsite.			
• If backups do not pass the validation and integrity checks a fresh copy of the database is made immediately to save a copy of the month's data			
The database is backed up prior to conducting restore			
The laboratory has a documented strategy to recover from database corruption			

Disaster Recovery Plan

Item	Yes	No	Comment
There are policies in place to validate the laboratory's disaster recovery process that specify:			
• What triggers the emergency protocol to be enacted			
• The duration and extent of required IT support			
The laboratory has the ability to anticipate the length of time it will take for data recovery			
The laboratory has a plan in place to maintain operations in the case of data loss or downtime			
The laboratory utilizes a fireproof safe to store data back-ups and/or maintains storage of back-up data off-site			
• These back-ups are accessible by the laboratory			
The laboratory has documented procedures to protect lab-defined essential data and prevent the loss of test result data in the event of equipment failure and/or an unexpected destructive event, such as fire or flood			
• This includes a set of instructions on how to recover the system			

Resources

Item	Yes	No	Comment
There is a facility system admin or trained super user responsible for completing LIMS backups and copying it to another location			
There is dedicated and fully functional IT support available during business hours			
At least two employees have administrative rights to the backup and recovery system			

There is an LIS Support team in place to monitor the backups remotely to ensure that backups are running and are being copied to external storages.			
• The team also monitors replication at sites where it has been configured.			
Lab managers or IT personnel are responsible for copying backups to an external media for safe storage onsite.			

Inventory

Item	Yes	No	Comment
The laboratory has created an electronic list of all media being used for backup and updates and verifies this list regularly.			
The laboratory has created an inventory of where all information lives.			

Test Recovery Procedures

Item	Yes	No	Comment
The laboratory conducts weekly checks to ensure data are being written to media correctly.			
The data needed for full recovery are available and can be accessed as needed.			
There is documentation to verify the most recent testing of backup.			

Frequency

Item	Yes	No	Comment
Backups 0- 30 days (Monthly)			
• All backups carried out during the last 30 days are retained and stored on the media device.			
• A copy of the week's data is stored offsite every weekend			
Backups (30-180 Days)			
• Two copies of the database are retained for bi-weekly. The two copies shall be retained on-site and offsite preferably at the APHL offices for safe keeping			
Backups (Greater than 6 Months)			
• A copy of the database is maintained for the end of each month both onsite and offsite. This will ideally contain changes made up to the end of that month.			

Backup Hardware

Item	Yes	No	Comment
If the laboratory uses external hard drives, flash drives, or tapes to conduct backups, they always have at least two available for storing the backups.			
Automatic network backups are scheduled daily, outside of working hours, and are sent to at least two different physical locations.			

Association of Public Health Laboratories

The Association of Public Health Laboratories (APHL) works to strengthen laboratory systems serving the public's health in the US and globally. APHL's member laboratories protect the public's health by monitoring and detecting infectious and foodborne diseases, environmental contaminants, terrorist agents, genetic disorders in newborns and other diverse health threats.

This project was 100% funded with federal funds from a federal program of $8.7 million. This publication was supported by Cooperative Agreement #U2GGH001097 from the US Centers for Disease Control and Prevention (CDC). Its contents are solely the responsibility of the authors and do not necessarily represent the official views of CDC or the Department of Health and Human Services.

8515 Georgia Avenue, Suite 700
Silver Spring, MD 20910
Phone: 240.485.2745
Fax: 240.485.2700
www.aphl.org