**Podcast Transcript: Information Management**

**Slide 1**: **Information Management QSE**

Hello-my name is Darla Schletty and I am the Security Administrator and Software Quality Coordinator at Mayo Clinic.

**Slide 2**: **User Access Security**

The first topic that we would like to cover as part of the Information Management Quality System Essential is User Access Security.

**Slide 3**: **System Access Request**

In order to comply with good Security practices, you need the ability to authenticate and authorize the users of the applications being used by your facility.

Authentication verifies *who you are.*

Authorization verifies *what you are authorized to do*.

To authenticate a user, there are various methods accepted in the industry. No matter what your company chooses to use, the authentication step must verify and confirm the user logging into the application/server, is who they say they are. A very common form of authentication is multi-factor authentication or MFA. MFA could be a password, token or even biometrics that are used to authenticate the user.

Once you have been authenticated, you now have the authorization in order to move throughout the application. What permissions should be granted to the user? A standard rule of thumb is that the user shouldn’t be allowed any more access than what their job necessitates. Policies should be put into place in order to standardize what type of authentication and authorization your company will be using.

**Slide 4: Role-Based Access Control**

Role based access control is a form or method of *authorization*. Assigning roles to employees will assure that the application is being used at the lowest level or the “need to know’ level in order for them to do their job. Assigning an employee to a profile or a birthright assures that each employee assigned to that birthright will only be able to access what has been approved for their position.

**Slide 5**: **Password Management**

Password management is one of the most important aspects of identification management.

The strength of your password should be enhanced by using a number of characters. Obviously, the password should not be easily guessed. When choosing a new password, a caution that I like to share is to never use a name of a person or a pet that lives in your house. We are human; and we like to talk about ourselves, our families and our pets. These types of passwords are commonly hacked.

One last recommendation for a secure password is to think of a sentence and choose the first letter of each word in that sentence. For example, ‘My Grandma's name is Toots. The password would be MGNIT. For those applications that require minimum characters, add numbers or characters to the password to meet the tool standards.

If you are struggling with your password entry, many applications are designed to ‘lock’ out the user after so many attempts. This would require administration intervention before allowing the user back into the tool. This lockout will prevent robots attempting to hack into an application. Policies should be in place to standardize password management.

**Slide 6: User Access Audit**

Now that the employees have access to applications within your business, a review of the application is a good standard, and depending on your business it may be a regulatory requirement. The audit of the user’s access will allow the System Administrators to confirm that the employees using the systems have had their role or permissions reviewed by their supervisor or designee.

Frequencies of the audits are sometimes mandated by regulations that your lab needs to adhere to. The frequency should be documented in a policy.

In order to accomplish the audit, you need to determine the parties involved in the access audit and what their role will be during the audit. Typically this is a System Manager, Supervisor and Access Security Officer.

A few other considerations for the access audit would be:

a. What information will be provided for the review?

b. What form of communication will be used to perform the audit?

c. What is the method of documenting the responses?

d. Will a spreadsheet be used to capture the responses or can a supervisor reply by email?

**Slide 7**: **Example of User Access List**

This is an example of a spreadsheet used for an access audit. In order to perform the user access audit, you must know who has access to the application or tool. The System Manager should provide a user access list.

Once the user list is generated, determine the supervisors affected by the review. Communication should be sent out to the affected supervisors including the list of the access being audited, the timeline for the audit, and their responsibilities during the audit.

A few additional details that should be included in the access audit policy:

a. If a response is ‘approved’ is there any additional steps to be taken?

b. If a user is instructed to be revoked, who will revoke their access and how will it be

documented?

c. And finally, what is the process for the reviewer if they identify an employee who no longer

works in their department?

In order to comply with regulatory requirements, you should have a policy in place that discusses how long the access audit records are retained.

**End segment**

**Slide 8**: **System Downtime**

Hello, my name is Mary Vehrenkamp and I am a Software Quality Analyst at the Mayo Clinic.

The second element that I would like to discuss as part of the Information Management Quality System Essential is System Downtime. System Downtime can be referenced in different ways. You may hear the terms Contingency Plan or IT Outage. All of these terms refer to the situation where the computer system is not available.

This is a very important topic for laboratory operations. Obviously, Information Technology or IT plays a role in managing system outages. During this discussion we will focus on **the laboratory’s responsibility** when the laboratory information system is not *available* (truncated).

**Slide 9**: **System Downtime**

Our computer systems are critical to the work that we do every day in the laboratory. We rely on our computer systems to:

* Track our specimens
* Order and result our tests
* Communicate test information to the providers
* Print patient reports
* Generate management reports, to list a few.

The regulatory and accreditation agencies that oversee our laboratories expect us to have documented plans in place to ensure that patient care is not adversely impacted during a system interruption.

Would you be able to answer the final bullet on this slide? – *How would laboratory operations continue in your laboratory if the information system was not available?*

**Slide 10**: **Illustration of News Bulletin**

System Downtime is not just critical for laboratory operations. It impacts your entire organization. Many people rely on laboratory test results. The communication process that you have in place is critical to your Downtime Plan. How do you communicate system downtime at your facility? This slide is an example of an alert message that could be published on your organization’s internal website to give specific information regarding an outage.

**Slide 11**: **Illustration System Status Panel**

Another way to communicate System Downtime is by using a System Status Panel. It provides your organization a quick view of the availability of critical clinical applications, including laboratory information systems.

As you can see in this example, there is a color key indicating the status. For example, **Blue** would mean that we have a system that is scheduled to undergo an outage at a future date, whereas **Red** indicates a system that is currently not functioning whatsoever.

**Slide 12: IT Outage Contingency Plan**

There can be different ways to document a System Downtime Plan for your laboratory. Laboratories and hospitals are required to have an Emergency Preparedness Plan to ensure we have effective responses in place to emergencies in order to protect our staff, patients and visitors. Emergency Preparedness Plans include responses for such events as:

* Evacuation
* Fire
* Weather and
* Medical Emergencies

You can incorporate a section within your Emergency Preparedness Plan to cover how you will manage an IT Outage. Another way to document a Laboratory System Downtime Plan would be to write a standard operating procedure that describes how your laboratory manages a system outage.

Whichever method you decide to use, it is **critical that staff is trained to** the System Downtime Plan and that they have had an opportunity to practice the elements of the plan. Staff will be more confident during a “real” outage if they have had the opportunity to demonstrate and practice what they have learned.

**Slide 13**: **Elements to Consider**

As you think about writing a System Downtime Plan, there are several elements you should consider. These elements may or may not be applicable to your laboratory but they should be thought through as you develop your plan.

Communication is critical during a system outage. How will laboratory staff respond? Who do they contact if they identify a problem with the laboratory system? What happens during off shifts? Who communicates to areas outside the laboratory that rely on laboratory test results?

Another critical topic to address is how specimens will be managed when they arrive in the laboratory. How will specimens be labeled appropriately? What information must be on the label if it is handwritten? How will priority or STAT specimens be identified and sorted? When and how will the laboratory stabilize specimens? Can the specimens stay at room temperature or should they be refrigerated or frozen?

**Slide 14: Elements to Consider**

Your System Downtime Plan also must assess the type of testing your laboratory performs and determine which tests will be run and which tests will be held until the system becomes available.

If you are a laboratory that performs STAT testing, your tolerance for waiting is diminished. You must implement alternate processes for testing and reporting so that you do not compromise patient care and continue to report results in a timely fashion.

For all laboratory testing, the laboratory should have manual backup forms in place to document test results until the laboratory information system becomes available. An example of a back-up form is included in the Resource section of this presentation.

**Slide 15**: **System Downtime Plan**

Your Downtime Plan does not end when the computer system becomes available. There is additional work that must be done. Testing that was performed and documented hardcopy now must be entered into the computer system. Identify who is responsible for this task. Manually entered results need to be verified by a second technologist to confirm accuracy. This should also be outlined in your plan.

In addition, the laboratory has a responsibility to ensure that data was not compromised when the system went down. As indicated in this slide, one option to confirm data integrity might be to review a sampling of patient test results and check the lab system as well as downstream systems to ensure accuracy.

If the testing was run on an instrument, you could review instrument printouts with results in the lab system and your electronic medical record. The LIS Outage Worksheet contained within the Resource materials provides you with an example of how your laboratory might document data integrity checks following a system outage.

**Slide 16**: **Thank you for listening.**

Thank you for listening. The podcast is completed. Please select the next button to continue.

**End podcast**