Cybersicherheit – bewährte Praktiken

Da sich die Risiken im Bereich der Cybersicherheit ständig verändern, ist ein präventiver Ansatz zur Sicherung von Labordaten von entscheidender Bedeutung.

Empfehlungen und bewährte Praktiken müssen an die Arbeitsumgebung im Labor angepasst und entsprechend den örtlichen Vorschriften und Praktiken abgeändert oder ergänzt werden.

1 Erforderliche Arbeitsumgebung

Software	STart Max Software 1.7.15 oder höher
Arbeitsplatz	Das Gerät kann an einen Stago-Arbeitsplatz angeschlossen werden (z. B. STA Coag Expert).
Kommunikation	Serielle RS232-Schnittstelle: Kommunikation mit dem LIS (ASTM-Protokoll) oder dem Arbeitsplatz (sofern zutreffend)
Videoübertragung	Touchscreen
Drucker	Ein Drucker kann lokal an das Gerät angeschlossen werden.
Benutzer	Stago-Systeme erfordern ein Benutzertraining.
Standort	Das System muss sich in einem Bereich mit eingeschränktem Zugang befinden, der vom Labor kontrolliert wird.

Bitte wenden Sie sich an einen Stago-Vertreter, falls Sie ein Systemupgrade benötigen.

2 Bewährte Praktiken

2.1 Schutz der Anschlüsse

2.1.1 Überprüfen Sie Wechseldatenträger vor der Verwendung

Aus technischen Gründen können Stago-Systeme nicht dauerhaft mit Antivirusprogrammen ausgestattet werden.

Alle USB-Sticks und andere Wechseldatenträger müssen auf einem PC mit einem aktuellen Antivirusprogramm überprüft werden, bevor sie mit dem Gerät oder dem Arbeitsplatz verbunden werden. Idealerweise sollte diese Überprüfung auf einem eigens dafür vorgesehenen Computer (mit aktuellem Antivirusprogramm ausgestattete separate Station) erfolgen.

Wir empfehlen, jedem Stago-Arbeitsplatz und -Gerät einen Wechseldatenträger zuzuweisen.

2.1.2 Überprüfen Sie Wechseldatenträger nach der Verwendung

Wir empfehlen, Wechseldatenträger auch nach der Verwendung zu überprüfen.

Wenn bei der Überprüfung ein Virus oder eine andere Schadsoftware festgestellt wird, brechen Sie die Verwendung des Geräts und des Arbeitsplatzes/Geräts sofort ab. Befolgen Sie das im Labor geltende Vorgehen und wenden Sie sich umgehend an den autorisierten örtlichen Stago-Kundendienstvertreter.

2.1.3 Verwenden Sie die USB-Anschlüsse ausschließlich für zulässige Geräte

Die USB-Anschlüsse dürfen nur für Geräte verwendet werden, die mit dem System bereitgestellt wurden oder die als optionales Zubehör zum System erhältlich sind (Handbarcodescanner).

Die Verwendung anderer Geräte an diesen Anschlüssen ist strengstens untersagt. Zum Beispiel dürfen keine Smartphones an Stago-Systeme angeschlossen werden.

2.2 Sicherheit von Patientendaten

2.2.1 Pseudonymisieren Sie Patientendaten

Identifizieren Sie die Patienten nach Möglichkeit nur anhand ihrer Röhrchennummern. Die Verwendung personenbezogener Daten sollte auf das absolute Minimum beschränkt werden, das für den ordnungsgemäßen Betrieb des Labors erforderlich ist.

Stellen Sie sicher, dass vertrauliche Daten das Labor nicht ohne Ihre Zustimmung verlassen.

Zur Erinnerung: Alle Patientendaten können am Bildschirm angezeigt, ausgedruckt, gespeichert und an das LIS (Labor-Informationssystem) gesendet werden.

2.2.2 Löschen Sie die Patientendaten inklusive der zugehörigen Rückverfolgbarkeitsdaten

Vor einer Rückgabe oder eines Austauschs des Geräts müssen alle Patientendaten inklusive der zugehörigen Rückverfolgbarkeitsdaten vom Gerät gelöscht werden.

Sichern Sie die Rückverfolgbarkeitsdaten und löschen Sie sie nach der Datensicherung

Tippen Sie im Menü [**System**] auf [**Datensicherung**] und den Abschnitt [**Manuelle Sicherung**] und folgen Sie den nachstehenden Anweisungen zur Sicherung der Rückverfolgbarkeitsdaten.

- [**Start**]: Geben Sie „30/01/01“ ein (entspricht dem 30. Januar 1901 bzw. 2001).
- [**Ende (inbegriffen)**]: Geben Sie das heutige Datum ein.
- Wählen Sie die Option [**Daten nach Sicherung löschen**].
- Stecken Sie einen leeren USB-Stick ein und klicken Sie auf [**Exportieren**], um die Datensicherung zu starten.
- Warten Sie, bis die Meldung erscheint, dass die Datensicherung abgeschlossen ist.

Fingieren Sie Patientenergebnisse, um den tatsächlichen Verlauf zu löschen

Automatische Erstanforderung

Tippen Sie im Menü [**System**] auf [**Inku/Wert**] und den Abschnitt [**Identifikationsnummer des Patienten**] und folgen Sie den nachstehenden Anweisungen, um die automatische Erstanforderung der Patientenidentifikationsnummern zu konfigurieren:

- [**ID-Präfix**]: Lassen Sie das Feld leer bzw. den vorhandenen Wert unverändert.
- [**Inkr.**]: Geben Sie „1“ ein.
- [**Anzahl der Kanäle**]: Geben Sie „4“ ein.

Erstellen eines Verfahrens

Tippen Sie im Menü [**System**] auf [**Tests**] und suchen Sie ein Verfahren mit folgenden Einstellungen bzw. erstellen Sie ein Verfahren mit der Bezeichnung „M1“ und folgenden Einstellungen:

- Tippen Sie auf [**Analyse**]:
  - Die Option [**Doppelte Messungen**] ist deaktiviert.
  - Abschnitt [**Messwert**]: Setzen Sie die T1-Inkubation auf „0,0 Sek.“ und die T2-Inkubation auf „35 Sek.“.
- Tippen Sie auf [**Kalibration**]: Der Modus ist eine Rohkalibration.

Hinweis: Das Verfahren muss zu den Favoriten hinzugefügt werden.

Fingieren neuer Patientenergebnisse

Erstellen Sie im Fenster **[INKUBATION/MESSUNG]** vier Küvettenstreifen mit den folgenden Einstellungen:

➤ Wählen Sie das gerade erstellte Verfahren **M1**.

➤ Wählen Sie als Probentyp [**Patienten**].

➤ Testen Sie den ersten Streifen mit Wasser anstelle von Plasma (kein Plasma oder anderes Material verwenden).

✓ Nach circa 5 Sekunden wird für alle vier Ergebnisse ein Kugel-Fehler angezeigt.

➤ Wiederholen Sie dieses Vorgehen, bis 52 Ergebnisse (insgesamt 13 Streifen) vorliegen.

➤ Überprüfen Sie im Menü [**PATIENTEN - Ergebnisse**] in der Spalte [**Patienten-ID**], dass nur die Identifikationsnummern mit der zuvor eingestellten Erstanforderung vorliegen und für alle ein Fehler angezeigt wird.

Wiederholen Sie die in Abschnitt „Sichern Sie die Rückverfolgbarkeitsdaten und löschen Sie sie nach der Datensicherung “ beschriebenen Schritt, um die letzten Patientenergebnisse zu löschen.

2.3 Weitere Empfehlungen von Stago

Installieren Sie keine unautorisierte Software oder Patches ohne vorherige Zustimmung von Stago

Umgehen Sie keine von Stago eingerichteten Sicherheitsmaßnahmen

Die von Stago zum Schutz des Laborsystems und der personenbezogenen Daten eingerichteten Sicherheitsmaßnahmen dürfen nicht umgangen oder deaktiviert werden.