United Clinical Laboratories
205 Bluff St, Ste1, Dubuque, IA 52001-6979
Phone: 563.556.2010

M.E. Kurt-Mangold, MD
C.J. Leigh, MD
P.D. Spivey
D.D. Slagel, MD
T.G. Timmerman, MD
A.D. Vanderheyden, MD

UCL LabXchange Security Policy – User Agreement – 2020 – 2021

Principle: This security policy is limited to the usage of the UCL (United Clinical Laboratories) LabXchange application, developed by UCL for healthcare personnel in our community access to laboratory results for patient treatment, payment or healthcare operations activities in accordance with HIPAA regulations.

Usage: The UCL LabXchange application gives UCL clients access to laboratory results of their patients for the purposes of treatment, payment or health care operations activities, in accordance with HIPAA regulations; no other uses are intended or implied.

Responsibility: As with other personal health information handled by authorized individuals in your facility, your patient privacy policies are to be effectively enforced. Searches must be limited to only those patients being seen by the physicians and caregivers in your practice.

Security Policy: LabXchange has two ports of entry, SSL encrypted access via the Internet and an unencrypted portal through the Dubuque Healthcare Intranet. Only approved health care givers and health care organizations (including sanctioned State agencies) having a business relationship with United Clinical Laboratories, Inc. are granted access to personally identifiable laboratory test results.

Levels of Security:

1.) Physical Safeguards – Two levels

a. Level one protection is provided only to those organizations that have a physical connection to the Dubuque Healthcare Intranet.
b. Level two access to UCL LabXchange requires a client install; i.e., only those workstations where the UCL LabXchange has been installed as a resident application can access the system.

2.) Security Mechanisms – Three levels

a. In addition to the physical security constraints, only those caregivers approved by their managers are granted usernames and passwords to the system. A signed user agreement is required from each person granted access to LabXchange on an **annual basis**. Passwords require an update at the frequency of your internal organizations' policy..
   i. Active users are verified on an annual basis. No use in 12 months results in discontinuation of user access.

ii. Note – An auto-login feature is provided as a user convenience to select clients with dedicated workstations using the Intranet version; it does not breach or circumvent the requirement for having an approved username and password. This feature uses the Micro Soft Windows based username of the person logged on to the workstation to grant access to laboratory results. The username is checked against an authorization list internally. It is the responsibility of the organization requesting the auto-login function to implement policies and timeouts to ensure that users are required to log onto a given workstation with their approved username and password before accessing protected information.

b. Audit Logging is integrated into LabXchange to track who, what and when related to accessing laboratory results. Random audits are conducted on a routine basis and provided to each facility with active users for review of appropriate access. Audits may also be requested by indicating audit type: user access or patient access with requested date ranges. Requests can be sent to info_ucl@pa-ucl.com
   i. Note – Just as it is with phoned and paper laboratory reports, it is the user-organization's responsibility to assure that its employees are using the system appropriately with respect to privacy policies and procedures.

c. SSL Encryption: This level of security is utilized for those organizations requiring access via the Internet. Due to the additional time required to encrypt and decrypt messages, this format is typically deployed when Intranet access cannot be attained.

_____

Jason Burds, CIO; v 03252020

Acknowledgement/Authorization:

Organization:

_____

Manager Signature: _____ Date: _____

User printed Name: First

_____

MI

_____

Last

_____

User Signature: _____ Date: _____

Optional
Requested User ID: _____