Single Sign-On Security Implementation

Amy Nichols, *Manager of Client Systems*

June 2, 2017

In an ongoing effort to protect the privacy of our shared patients' protected health information, PathGroup has strengthened our security measures. Beginning **June 5, 2017**, all PathGroup electronic client systems including PathConnect, PathGroup Mobile, Result Review, PathSupply and AutoPrint will have a new Single Sign-On system that will strengthen the authentication access. PathGroup's new password procedures are required by all users.

The new Single Sign-On program will require more complex passwords, prevent password reuse, and will set limits for password expiration to every 60 days. If there has been no activity by a user within 60 days, their account will automatically be disabled. After an account is disabled, the user will receive a message upon attempted sign-on. They will need to contact PathGroup IT Support to start the process of re-enabling their account.

If additional user credentials are needed, please submit a Client Access Request Form that is completed and approved by an appropriate person.

Users will be notified of their upcoming password expiration 7 days prior to expiration. This notification will continue every day until the day of expiration.

New password requirements must be:
- Minimum of 8 characters
- Maximum of 25 characters
- Different from the 6 previous passwords
- Include at least 1 lower case letter and 1 upper case letter
- Include at least 1 number
- Include at least 1 special character

All PathGroup electronic client system users will need to sign the electronic PathGroup Security Agreement which will be presented at first sign-on after June 5, 2017. We thank you for joining us in implementing stronger protections of our patients' data.

For further questions, please contact your PathGroup Account Management representative.