IS SECURITY GUIDANCE

Emergency Access to Health Information During COVID-19

During normal operations, healthcare workers are provided only the access they need to support their job function. However, as essential workforce members are supporting the COVID-19 response, there may be policy exceptions which require the elevation of access for multiple groups of users. Note that this method of break the glass is not the EMR alert which users receive when accessing a sensitive part of a patient's record. The context of break the glass is the elevation of access of groups of users to support a mass casualty or public health event such as the COVID-19 response.

A well-designed break the glass process will reduce policy, operational, and technical barriers to patient information; which if not used, can cause more harm to the patient than the original safeguard. They should not be a work around when one user needs extra access, a co-worker is absent, or as a workaround for a poorly designed identity access management process. HIPAA still requires maintaining minimum necessary access, strong passwords, and audit and monitoring controls. Electronic prescriptions for controlled substances still require multi-factor authentication.

"BREAK THE GLASS" NEXT STEPS

1. Assemble your information technology and identity access management teams, clinical application SMEs, EMR vendor(s), privacy and security officials, and operations supervisors to co-design a Break the Glass policy and complementary process for system and database administrators, EMR administrators, and essential workforce users who will be assigned to Break the Glass security access.
2. Create policy exception justification for the use of BtG process.
    1. Transferring staff members to different department, role, or facility.
    2. Provisioning bulk remote workers.
    3. Information technology department requires additional system administrators to support an incident.
    4. Onboarding large groups of new workforce members to assist with response.
3. Consider requirements of providing bulk elevated access to using pre-staged roles, facilities, departments, and groups within Active Directory, remote VPN group, multi-factor authentication, and the critical applications in scope.
4. Create predetermined documented process with established criterion and approval process to activate BtG. (Think 2 -3 executive level approval like nuclear codes.)
5. Create criteria for activating the Break the Glass process and backend prewritten scripts to run upon activation of the BtG procedure to automate the process.
6. Extend audit trails with longer retention periods. Back up audit trails and include offsite from originating location.
7. Present design to leadership for approval.
8. Test the implementation and update issues.
9. Train all impacted workforce members on their role during BtG process.
10. Exercise the Break the Glass process.