

Information Privacy and Security Council  
*Proposed Best Practices and Guidelines for Handling Employee Health Information*

- Best efforts should be undertaken by all departments to ensure only appropriate and authorized staff view and/or handle employee health information. This is typically human resources and direct supervisors, as necessary.
- Access to the electronic health data must be limited to role-based functions (job functions).
- All employee health information must be secured during transit (both physical and electronic). When transporting hard-copy materials within the office, said materials must be placed in an envelope labeled with the employee's name. If transported between office locations, the envelop must be marked "Confidential."
- Data at rest in electronic systems must be secured by encryption.
- With the exception of family and medical leave and/or workers' compensation records maintained by authorized human resources personnel, the practice of attaching doctors' notes to leave request forms (e.g., state form "G-1") should cease. Alternatively, it is sufficient for a supervisor to verify that a doctor's note was presented by the employee (e.g., revised G-1 eSign so that supervisor has option to select "Doctor's note presented on [date]."