

# FORM 5

## COMPLIANCE PLAN PROVISIONS

HIPAA requires that physicians' compliance plans contain the following elements to ensure HIPAA's administrative requirements are adhered to by the physician's practice. The compliance plan must:

1. Designate and document the designation of a privacy official to develop and implement HIPAA's policies and procedures. A person must also be designated as a contact person responsible for receiving complaints and responding to questions regarding the Notice of Privacy Practices and such designation must be documented.
2. Train and document the training of all employees regarding HIPAA's privacy rules. Training must also be provided within a reasonable time after new employees begin work.
3. Have in place appropriate administrative, technical and physical safeguards to protect the privacy of medical information.
4. Institute and maintain a process for individuals to make complaints regarding the practice's implementation of the HIPAA privacy rules. All such complaints and their disposition must be documented.
5. Apply and document sanctions against employees who violate HIPAA's privacy rules.
6. Mitigate harmful effects of violations of HIPAA's privacy rules by the practice or its Business Associates.
7. Not discriminate, threaten, intimidate or otherwise take retaliatory actions against any patient or employee exercising their rights provided by HIPAA's privacy rules.
8. Institute and document policies and procedures to comply with HIPAA's privacy rules, taking into account the practice's size and activities.
9. Retain all documentation regarding compliance with HIPAA's privacy rules for six years after the date the information was created or was last in effect.