Keeping Client Information Private & Secure

DSHS is required by state and federal law to protect and maintain the privacy and security of confidential client information.

Federal privacy laws that we may be subject to include:

- the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and corresponding regulations at 42 C.F.R. Parts 160 and 164;
- Substance Abuse Confidentiality Regulations 42 C.F.R. Part 2 Revised (2011);
- the Federal Privacy Act of 1974; and
- the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, and corresponding regulations at 34 C.F.R. Part 99

When contractors have access to confidential client information, we must also require them to safeguard the privacy and security of our clients' confidential data.

Your contract with DSHS contains several important provisions intended to safeguard and protect the privacy of DSHS clients' confidential information, including protected health information (PHI). These contract provisions may include:

- the ***Confidentiality*** section of the General Terms & Conditions
- the **HIPAA Compliance/Business Associate** section
- the **Data Security Requirements Exhibit**

If you subcontract any portion of the services provided under your contract, you must also ensure that your subcontractors are also following all the relevant data security and confidentiality provisions that are included in your contract.

This means you must include the same requirements found in your contract with DSHS in your contracts with your subcontractors.

You must also **obtain approval from DSHS in advance before you subcontract** out any of the services under your contract. If your contract does not explicitly state that you have approval to subcontract, then you must contact the DSHS Contact identified on the face sheet of your contract to obtain DSHS approval **before** you subcontract any services out.