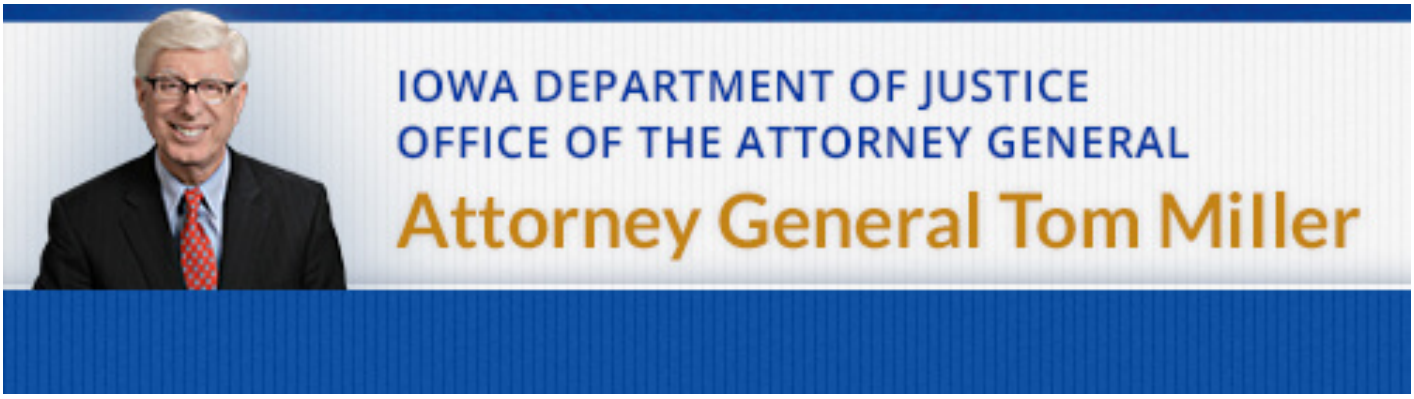


# Confidentiality and Safety

Each agency that receives a grant from the Crime Victim Assistance Division (CVAD) to provide direct services to victims of crime must have a confidentiality policy in place to protect confidential, personally identifying information. At minimum, this policy should include a description of informed consent, a description of any circumstances in which a program would release confidential information, as well as steps to be taken by the agency in the event of a breach, or release of personally identifying information (whether intentional or accidental). Furthermore, a confidentiality assurance should be signed by all staff, volunteers, interns, board members and anyone else who could potentially have contact with survivors. At a minimum, the policy should state the individual will protect the personally identifying information of all persons contacting the agency for service, regardless of whether these persons actually receive services from the agency.

**Under no circumstances should any victim of crime be required to provide consent to release personally identifying information as a condition of eligibility for the services provided by the grantee or subrecipient.**

Informed consent means giving a survivor information about who will be receiving the information, the expected purpose of the release and any potential dangers or negative outcomes of releasing information, if known.

Personally identifying information or personal information means individually identifying information for or about an individual including anything likely to disclose the location of a victim, including but not limited to:

- First and last name;
- Home or other physical address;
- Contact information (including, but not limited to, email address, telephone/fax number, web address or postal address);
- Social security number
- Driver’s license number
- Passport number
- Student identification number; and
- Any other information including date of birth, racial or ethnic background, or religious affiliation that would serve to identify an individual.

**Agencies should ensure all client information containing personally identifying information is kept out of view from other clients, visitors, volunteers and others who are not authorized to view the information. Furthermore, client records not in use should be stored in a secure area, locked cabinet, drawer or similar storage item. If client files are stored electronically, agencies must ensure appropriate security measures are taken to protect client data such as firewalls, authorized user accounts, password protection, etc.**