the disclosure of patient identifying information relating to the cause of death of a patient under laws requiring the collection of death or other vital statistics or permitting inquiry into the cause of death.

(2) *Consent by personal representative.* Any other disclosure of information identifying a deceased patient as having a substance use disorder is subject to the regulations in this part. If a written consent to the disclosure is required, that consent may be given by an executor, administrator, or other personal representative appointed under applicable state law. If there is no such applicable state law appointment, the consent may be given by the patient's spouse or, if none, by any responsible member of the patient's family.

[82 FR 6115, Jan. 18, 2017, as amended at 83 FR 251, Jan. 3, 2018]

§ 2.16 Security for records.

(a) The part 2 program or other lawful holder of patient identifying information must have in place formal policies and procedures to reasonably protect against unauthorized uses and disclosures of patient identifying information and to protect against reasonably anticipated threats or hazards to the security of patient identifying information. These formal policies and procedures must address:

(1) Paper records, including:

(i) Transferring and removing such records;

(ii) Destroying such records, including sanitizing the hard copy media associated with the paper printouts, to render the patient identifying information non-retrievable;

(iii) Maintaining such records in a secure room, locked file cabinet, safe, or other similar container, or storage facility when not in use;

(iv) Using and accessing workstations, secure rooms, locked file cabinets, safes, or other similar containers, and storage facilities that use or store such information; and

(v) Rendering patient identifying information non-identifiable in a manner that creates a very low risk of re-identification (*e.g.*, removing direct identifiers).

(2) Electronic records, including:

(i) Creating, receiving, maintaining, and transmitting such records;

(ii) Destroying such records, including sanitizing the electronic media on which such records are stored, to render the patient identifying information non-retrievable;

(iii) Using and accessing electronic records or other electronic media containing patient identifying information; and

(iv) Rendering the patient identifying information non-identifiable in a manner that creates a very low risk of re-identification (*e.g.*, removing direct identifiers).

(b) [Reserved]

§ 2.17 Undercover agents and informants.

(a) *Restrictions on placement.* Except as specifically authorized by a court order granted under § 2.67, no part 2 program may knowingly employ, or enroll as a patient, any undercover agent or informant.

(b) *Restriction on use of information.* No information obtained by an undercover agent or informant, whether or not that undercover agent or informant is placed in a part 2 program pursuant to an authorizing court order, may be used to criminally investigate or prosecute any patient.

§ 2.18 Restrictions on the use of identification cards.

No person may require any patient to carry in their immediate possession while away from the part 2 program premises any card or other object which would identify the patient as having a substance use disorder. This section does not prohibit a person from requiring patients to use or carry cards or other identification objects on the premises of a part 2 program.

§ 2.19 Disposition of records by discontinued programs.

(a) *General.* If a part 2 program discontinues operations or is taken over or acquired by another program, it must remove patient identifying information from its records or destroy its records, including sanitizing any associated hard copy or electronic media, to render the patient identifying information non-retrievable in a manner