(2) The minor applicant's situation poses a substantial threat to the life or physical well-being of the minor applicant or any other individual which may be reduced by communicating relevant facts to the minor's parent, guardian, or other individual authorized under state law to act in the minor's behalf.

§ 2.15 Incompetent and deceased patients.

(a) *Incompetent patients other than minors*—(1) *Adjudication of incompetence.* In the case of a patient who has been adjudicated as lacking the capacity, for any reason other than insufficient age, to manage their own affairs, any consent which is required under the regulations in this part may be given by the guardian or other individual authorized under state law to act in the patient's behalf.

(2) *No adjudication of incompetency.* In the case of a patient, other than a minor or one who has been adjudicated incompetent, that for any period suffers from a medical condition that prevents knowing or effective action on their own behalf, the part 2 program director may exercise the right of the patient to consent to a disclosure under subpart C of this part for the sole purpose of obtaining payment for services from a third-party payer.

(b) *Deceased patients*—(1) *Vital statistics.* These regulations do not restrict 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]