

Commission on Dental Accreditation

Privacy and Data Security Requirements for Institutions

(Rev. 9/7/17)

1. **Sensitive Information.** To protect the privacy of individuals and to comply with applicable law, the Commission on Dental Accreditation (“CODA” or “the Commission”) **prohibits all programs/institutions from disclosing in electronic or hard copy documents** provided to CODA other than on-site during a site visit, any of the following information (“Sensitive Information” or “PII”):
 - Social Security number
 - Credit or debit card number or other information (e.g., expiration date, security code)
 - Drivers’ license number
 - Account number with a pin or security code that permits access
 - Health insurance information, such as policy number or subscriber I.D.
 - Medical information, such as information about an individual’s condition or treatment
 - Mother’s maiden name
 - Taxpayer ID number
 - Date of birth
 - Any data protected by applicable law (e.g., HIPAA, state data security law)
 - Biometric data, such as fingerprint or retina image
 - Username or email address, in combination with a password or security question that permits access to an online account

2. **Patient Identifiers.** Before submitting information about a patient to CODA other than on-site during a site visit, a program/institution **must remove the following data elements** of the individual, and of relatives, household members, and employers of the individual (the “Patient Identifiers”):
 1. Names, including initials
 2. Address (including city, zip code, county, precinct)
 3. Dates, including treatment date, admission date, age, date of birth, or date of death [a range of dates (e.g., May 1 – 31, 2015) is permitted provided such range cannot be used to identify the individual who is the subject of the information]
 4. Telephone numbers
 5. Fax numbers
 6. E-mail addresses
 7. Social Security numbers
 8. Medical record numbers
 9. Health plan beneficiary numbers
 10. Account numbers
 11. Certificate/license numbers
 12. Vehicle identifiers and serial numbers, including license plate numbers
 13. Device identifiers and serial numbers
 14. Web Universal Resource Locators (URLs)
 15. Internet Protocol (IP) address numbers
 16. Biometric identifiers (e.g., finger and voice prints)
 17. Full face photographic images and comparable images
 18. Any other unique identifying number, characteristic, or code:

- that is derived from information about the individual
- that is capable of being translated so as to identify the individual, or
- if the mechanism for re-identification (e.g., the key) is also disclosed

In addition, the information provided to CODA cannot be capable of being used alone or in combination with other information to identify the individual.

3. **Redaction.** When removing any Sensitive Information or Patient Identifier from paper or electronic documents disclosed to CODA, programs/institutions shall **fully and appropriately** remove the data such that the data cannot be read or otherwise reconstructed. Covering data with ink is not an appropriate means of removing data from a hard copy document and may sometimes be viewable when such documents are scanned to an electronic format.
4. **Penalty fee.** *If the program/institution submits any documentation that does not comply with the directives noted above, CODA will assess a penalty fee of \$1000 to the program/institution; a resubmission that continues to contain prohibited data will be assessed an additional \$1000 fee.*
 - CODA Site Visitors and Commission volunteers are only authorized to access Sensitive Information and Patient Identifiers:
 - Onsite during a site visit, and
 - That are necessary for conducting the accreditation site visit
 - CODA Site Visitors and Commission volunteers may not download or make hard copies or electronic copies of Sensitive Information or Patient Identifiers.

NOTE: If a document includes fictitious information, which may otherwise appear to be Sensitive Information or Patient Identifiers, the program is expected to clearly mark the document as “Fictitious Example”.