Standard 5: Preparing your de-identified Chart for submission to DEAP

You will be required to submit ONE completely de-identified patient chart from your electronic or paper medical record system for your initial and renewal applications. If you are selected for an audit at any time during your accreditation term, you will be required to submit 5-10 de-identified charts.

The documentation of the DSMES intervention requested as part of your DEAP application should represent how you will document and communicate your DSMES services within your electronic or paper medical record.

You are providing a snapshot from one patient who has received diabetes education and support as part of your DSMES program and showing the entire intervention as “proof” that you are meeting Standard 5: Person Centered DSMES. Use our DEAP Chart Audit tool as a reference to be sure you have included each required component in your DSMES chart record.
PHI: Protected Health Information

Your chart must be completely de-identified and must not contain PHI. As a healthcare provider, you must adhere to HIPAA guidelines; if a chart is submitted to DEAP containing any PHI, it will be immediately deleted. Submitting documents that include any PHI will result in deletion of the document from your application. You will be required to re-submit the document with all PHI removed, ultimately delaying the approval of your application. The following list was obtained from https://compliancy-group.com/protected-health-information-understanding-phi/ accessed on 5/11/23

1. Name
2. Address (including subdivisions smaller than state such as street address, city, county, or zip code)
3. Any dates (except years) that are directly related to an individual, including birthday, date of admission or discharge, date of death, or the exact age of individuals older than 89
4. Telephone number
5. Fax number
6. Email address
7. Social Security number
8. Medical record number
9. Health plan beneficiary number
10. Account number
11. Certificate/license number
12. Vehicle identifiers, serial numbers, or license plate numbers
13. Device identifiers or serial numbers
14. Web URLs
15. IP address
16. Biometric identifiers such as fingerprints or voice prints
17. Full-face photos
18. Any other unique identifying numbers, characteristics, or codes

Please also reference https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected