

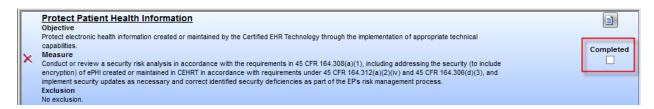
ONCOCHART protects health information using some of the following methods: audit trailing user activity, enforcing an inactivity timeout, limiting the number of login attempts, enforcing a minimum password length and restricting password reuse.

How to meet this measure -

Have your IT/security department conduct a security audit based on the requirements under $\underline{45}$ CFR $\underline{164.308(a)(1)}$, , including addressing the security (to include encryption) of ePHI created or maintained in CEHRT in accordance with requirements under 45 CFR $\underline{164.312(a)(2)(iv)}$ and 45 CFR $\underline{164.306(d)(3)}$, and implement security updates as necessary and correct identified security deficiencies as part of the EP's risk management process.

This HealthIT.gov <u>Security Risk Assessment</u> website link should prove to be a very useful resource for you regarding this measure.

Once you've completed the requirements of this measure, you'll need to manually check the *Completed* checkbox in the MU calculator. Retain the proof of this assessment in case of an audit.



Notes

If you wish to set up the inactivity minute security feature in ONCOCHART, contact <u>ONCOCHART</u> <u>Support</u> for instructions. This will need to be enabled at the individual computer level.

Myth vs Fact

Myth - My EHR vendor took care of everything I need to do about privacy and security.

Fact - False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.

Myth - My security risk analysis only needs to look at my HER.

Fact - False. Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone). Remember that <u>copiers also</u> store data.

Reviewed and modified on 4/27/2016 This document is the property of BMSi, Inc, and it for the sole use of the intended recipient(s) and may contain classified, proprietary, confidential, trade secret or privileged information. Any unauthorized review, use, disclosure or distribution is prohibited and may be a violation of law.