

Certification/Adoption WG

Discussion of CEHRT Definition Recommendations

April 27, 2012

Summary: 2014 Edition Definition of CEHRT

Builds on modular approach defined in 2011 Edition but allows EPs and EHs to tailor CEHRT to meet their individual needs

- Base EHR as common foundation for all with modular components added on top according to Core and Menu objectives being pursued

Implications for providers

- Does not force purchase of unnecessary modules
- May place greater burden on providers to assess quality of integration of disparate modules
 - Biggest area of concern is privacy & security
 - Modules no longer required to meet P&S requirements because they are included in Base EHR
 - Lack of requirements or guidance on integration of modules with Base and with each other could leave gaps in security, safety, and usability

Implications for vendors

- Could reduce demand for Complete EHRs since providers no longer required to purchase technology that meets all Core and Menu requirements
 - Depends on degree of integration challenges and provider willingness to anticipate need for additional modules beyond Stage 2
- Creates incentives for integrated solution packages focused on particular specialties and EP/EH segments – could be a long period of market experimentation before stabilization however
- Could increase demand for best-of-breed modules and for module integration technologies

Overall market impact

- Unclear – providers may still feel compelled to purchase complete EHR systems if integration challenges affect security, safety, and usability of systems

Recommendation: Voluntary Base EHR Integration Certification

Recommendation: Certification/Adoption WG supports ONC the 2014 Edition approach to CEHRT. However, the WG recommends that ONC add a Voluntary Base EHR certification specification to test integration of Base modules with respect to security, safety, and usability.

For

- WG appreciates challenge of testing integration – difficult to define integration parameters, and impractical to test all possible combinations of modules
- However, we are concerned that complete lack of integration guidance and testing could place too large a burden on providers
 - Can only truly assess level of integration after purchases are made, when it's too late to remedy
 - Many providers will be unable to assess robustness of security integration on their own
 - Market could develop on its own, but even if it did, would almost certainly happen too late to meet Stage 2 needs
- Voluntary Base EHR certification would be a compromise approach
 - Provides incentive to market to develop integrated Base EHR packages
 - Gives greater set of validated packaged choices to providers who otherwise could only choose a Complete EHR

Against

- Too difficult to define measureable, objective parameters of usability
- Supply-side will respond if there is demand for Base EHR integration (or any other well-articulated collections of modules)
- Certification bodies have not been required to test integration in past – would have to build new processes and capacities

Recommendation: Voluntary Security Integration Certification

Recommendation: Certification/Adoption WG supports ONC the 2014 Edition approach to CEHRT. However, the WG recommends that ONC add a voluntary Security integration certification specification to test integration of Base, Core, or Menu modules with security module contained in Base EHR.

For

- WG appreciates challenge of testing integration – difficult to define integration parameters, and impractical to test all possible combinations of modules
- However, we are concerned that complete lack of integration guidance and testing could place too large a burden on providers
 - Many providers will be unable to assess robustness of security integration on their own
 - Market could develop on its own, but even if it did, would almost certainly happen too late to meet Stage 2 needs
- Voluntary Security integration certification would be a compromise approach
 - Provides incentive to market to develop modules integrated with Base security modules
 - Allows more choice to providers without capability or desire to assess security integration on their own
 - Allows more sophisticated providers flexibility to take integration responsibility on their own

Against

- Too difficult to define measureable, objective parameters of security integration
- Supply-side will respond if there is demand for security integration
- Certification bodies have not been required to test security integration across modules in past – would have to build new processes and capacities
- Could end up forcing many module vendors to meet security requirements, which goes against 2014 Edition intent to lower barriers to entry for modular approaches