#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	0. Information Security Management Program
1	Centura Health	Kris Kistler		5	207-215	2.1	Please keep. The Framework Core Functions are an excellent identification of functional elements of an information security program or management system (ISMS).	Please keep the core functions of Identify, Protect, Detect, Respond, and Recover.
2	Centura Health	Kris Kistler		6	224-226	2.1	The Categories should change to correlate with the HITRUST CSF categories.	The Categories would be best served by using the existing HITRUST Common Security Framework (CSF) Categories that are closely aligned with ISO-27001: 0. Information Security Management Program 1. Access Control 2. Human Resources Security 3. Risk Management 4. Security Policy 5. Organization of Information Security 6. Compliance 7. Asset Management 8. Physical and Environmental Security 9. Communications and Operations Management 10. Information Systems Acquisition, Development and Maintenance 11. Information Security Incident Management 12. Business Continuity Management http://hitrustalliance.net

3	Centura Health	Kris Kistler		6	232-237	2.1	Informative references should mimic the HITRUST Authoritative sources and consist of already existing control references such as the ones listed. Controls should be cross-mapped to the various sources similar to the way HITRUST has done.	HITRUST CSF Authoritative sources: 201 CMR 17.00 State of Massachusetts Data Protection Act ISO/IEC 27001:2005 ISO/IEC 27002:2005 ISO/IEC 27799:2008 CMS Information Security ARS 2010 v1.0 COBIT 4.1 HIPAA (CFR part 164 Sections 308, 310, 312, 314 and 316) HITECH Act (CFR Parts 160 and 164) Encryption / Destruction Guidance (CFR parts 160 and 164 Federal Register 21 CFR Part 11 16 CFR Part 681 – Identity Theft Red Flags rules NIST Special Publication 800-53 Revision 3 NIST Special Publication 800-66 Payment Card Industry (PCI) DSS v2.0 Cloud Security Alliance (CSA) Cloud Controls Matrix v1 The Joint Commission (formerly Joint Commission on the Accreditation of Healthcare Organizations JCAHO) NRS: Chapter 603A – State of Nevada In addition to ISO-27001, NIST 800-53 and related documents, other ideal sources of best practices and standards are the SANS Institute top 20 critical security controls. http://www.sans.org/critical-security-controls/
4	Centura Health	Kris Kistler		9	321-389	2.4	The Framework Implementation Tier system should be replaced with the existing HITRUST PRISMA Maturity Model to measure program effectiveness.	Effectiveness should be measured by utilizing the HITRUST CSF Program Review for Information Security Management Assistance (PRISMA) maturity model available here: http://www.hitrustalliance.net/HITRUST%20Healthcare%20InfoSec%20Trends.pdf

5	Centura Health	Kris Kistler		13	457-492	Appendix A	The subcategory controls are too vague. More specific and directly auditable controls should be specified. Please reference HITRUST Controls and Control Elements	The subcategory controls are too vague. More specific and directly auditable controls should be specified. Please reference HITRUST Controls and Control Elements
6	Centura Health	Kris Kistler					We frequently struggle with vendors and exposures from their systems, especially in the biomedical device field. The framework should consistently require the same level of access controls, hardening, logging, and vulnerability remediation controls from any networked device.	Require Third Party Vendors, Business Partners, Bio-Medical and any other networked system to adhere to same requirements.

	Centura Health	Kris Kistler					Stronger Access Controls consistent with NIST 800-53 Level 3 controls should be enforced. Without two factor authentication, a physician's credentials could be compromised and used from any device or computer by any person. The two factor process significantly reduces the risk associated with this. A common method is to perform a "Man-in-the-Middle" attack, in which a device or virtual electronic spoof is made to insert a device or program in between the client and web server communication, allowing the encryption to be bypassed, and the physicians credentials exposed to the hacker who can then use them at will. A device purposefully made for just such attacks was recently released at the DefCon Hacker conference in July for $99. It sold out in hours. http://hakshop.myshopify.com/collections/gadgets http://blogs.computerworld.com/19671/sneak_pineapple_peak_hak5_creates_even_more_lethal_wi_fi_hot_spot_honeypot_hacking_tool The most likely initial compromises will be of individual patient accounts due to phishing attacks, or keystroke logging on the patient's personal accounts and systems. Targeted attacks (spearphishing) could result in larger numbers of these	Two factor authentication is recommended as a requirement for any external (internet) system access. A compromised patient account would normally only provide access to a single patient record, but if underlying existing or future flaws are exploited, it could lead to thousands of compromised patient records. In the past year, the threat landscape has increased significantly for healthcare organizations, partly due to the healthcare.gov deficiencies making news headlines. New hacker tools have been released in the last year that also increase the risk for man-in-the-middle and phishing attacks to be successful by lower level hackers and teenagers.
8	Centura Health	Kris Kistler					Simply utilize existing HITRUST Common Security Framework (CSF), which meets all desired objectives.	Adopt HITRUST Common Security Framework (CSF)