Detailed Content Outline

	Cognitive Levels			
	Recall	Application	Analysis	TOTAL
1. Privacy Standards, Policies, and Procedures	**3**	**10**	**4**	**17**
A. Define organizational and informational components subject to the program				
B. Review policies and procedures				
C. Propose governance policies related to the program (e.g., Board of Trustees, data governance, collaborative data sharing, HIEs)				
D. Ensure that a non-retaliation policy exists				
E. Develop policies and procedures				
F. Integrate mission, vision and values with code of conduct				
G. Maintain privacy program and work plan				
H. Consult with legal resources				
I. Ensure that a record retention policy exists				
J. Ensure maintenance of policies and procedures that address regulatory requirements (e.g., HIPAA Privacy and Security, HITECH, GLB Act, FERPA, GINA)				
K. Ensure maintenance of policies on interactions with other industry participants (e.g., hospitals/physicians, payors, information technology, vendors)				
L. Ensure maintenance of standards of accountability for employees at all levels				
M. Maintain communications and notices for stakeholders (e.g., privacy notices, GLB communications, FTC)				
2. Privacy Compliance Program Oversight	**3**	**10**	**3**	**16**
A. Review the responsibilities, purpose and function for program staff				
B. Ensure risk assessments are conducted				
C. Recommend the scope of the program				
D. Develop an annual work plan				
E. Participate in the development of internal controls				
F. Integrate the program into operations				
G. Ensure that the organization has defined the responsibilities, purpose, function and authority of the privacy officer				
H. Assure governance understands its responsibility as it relates to the program				
I. Ensure that the oversight committee's goals and functions are addressed				
J. Report program activity to the governance board/committee				
K. Coordinate operational aspects of the program with management				
L. Collaborate with others to institute best practices				
M. Coordinate organizational efforts to maintain the program				
N. Maintain knowledge of regulations and interpretation of laws				
O. Apply knowledge of regulations and interpretation of laws to emerging business practices and technologies				
P. Recognize the need for outside expertise				
Q. Manage an educational program				
R. Ensure that the role of counsel is clarified as it relates to the program				
S. Incorporate aspects of regulatory guidelines/enforcement into operations (e.g., OIG, OCR, FTC, HITECH)				
T. Ensure contracts include privacy elements when necessary				
U. Maintain the credibility and integrity of the program				
V. Evaluate the effectiveness of the program on an ongoing basis				

Detailed Content Outline

	Cognitive Levels			
	Recall	Application	Analysis	TOTAL
3. Screening/Evaluation of Employees, Physicians, Vendors and Other Agents	**3**	**5**	**1**	**9**
A. Include privacy obligations/responsibilities in job descriptions				
B. Include privacy compliance as an element in job evaluations				
C. Ensure background checks are conducted on personnel in accordance with applicable rules and laws				
D. Recommend that privacy-related issues are included in exit interviews				
E. Ensure due diligence on third party vendors (e.g., BAAs, subcontracts, data use agreements, collaborative data sharing arrangements)				
4. Communication, Education, and Training on Compliance Issues	**4**	**11**	**2**	**17**
A. Distill complex laws and regulations into understandable formats				
B. Develop role-based training programs				
C. Provide education on privacy policies				
D. Ensure general privacy training is conducted (e.g., employees, physicians, vendors, and other agents)				
E. Conduct risk-specific training for targeted individuals or groups				
F. Ensure participation in ongoing privacy training programs is tracked				
G. Disseminate guidance/regulatory materials				
H. Communicate privacy information throughout the organization				
I. Assure that individuals understand their documentation obligations related to privacy				
J. Ensure that a process exists so that individuals understand the privacy aspects of their role				
K. Promote an organizational culture that values the protection of sensitive information				
L. Encourage employees to seek guidance and clarification when in doubt				
M. Participate in continuing education to maintain professional competence				
5. Privacy Monitoring, Auditing, and Internal Reporting Systems	**3**	**4**	**10**	**17**
A. Conduct organizational risk assessments				
B. Develop plans of action based on risk priorities				
C. Develop an annual auditing and monitoring plan				
D. Ensure that auditing and monitoring tools exist				
E. Conduct audits				
F. Monitor for violations of laws and regulations				
G. Monitor audit results (e.g., track, trend, evaluate, benchmark)				
H. Perform ongoing monitoring (e.g., high risk priorities, policies and procedures, regulatory requirements)				
I. Operate system(s) to enable individuals to report noncompliance (e.g., hotline, open-door policy, drop box, anonymous mechanisms)				
J. Publicize the reporting system to all employees, physicians, vendors, and others				
K. Protect anonymity and confidentiality within legal and practical limits				
L. Ensure investigations are conducted independently of the operational unit				
M. Address concerns expressed by individuals through internal reporting				

Detailed Content Outline

	Cognitive Levels			
	Recall	Application	Analysis	TOTAL
N. Monitor internal reporting results (e.g., track, trend, evaluate, benchmark)				
O. Address audits conducted by external entities				
6. Discipline for Non-Compliance	**2**	**5**	**2**	**9**
A. Ensure that privacy violations are addressed in disciplinary policies				
B. Coordinate with management to ensure corrective action is taken				
C. Recommend disciplinary action proportionate to violation when noncompliance is substantiated				
D. Monitor disciplinary actions throughout all levels of the organization (e.g., consistency, type of violation)				
E. Ensure disciplinary action is documented				
7. Investigations and Remedial Measures	**2**	**7**	**6**	**15**
A. Respond to inquiries promptly, thoroughly, and discretely				
B. Conduct fair, objective, and discrete investigations				
C. Coordinate investigations to preserve defined privileges (e.g., attorney client, peer review)				
D. Investigate matters related to noncompliance				
E. Communicate noncompliance through defined channels				
F. Ensure corrective action plans are developed in response to noncompliance				
G. Incorporate changes to privacy program to reduce risk				
H. Maintain records on compliance investigations				
I. Monitor the effectiveness of corrective action plans				
J. Initiate policies and/or education to respond to identified problems or vulnerabilities				
K. Ensure coordination of data breach responses				
L. Ensure disclosure notification requirements are identified				
M. Ensure required notifications occur				
N. Participate in interactions with regulatory agencies (e.g., negotiations, inquiries, clarifications)				
O. Assure investigation personnel have the necessary skill sets				
P. Institute immediate measures as necessary to mitigate ongoing harm				
Totals	**20**	**52**	**28**	**100**

Answer key for page 21				
1.B	2.A	3.A	4.C	5.C