The Clearwater HIPAA and NIST-based Cyber Risk Management BootCamp™ comprises:

I. April 24, 2018 - 1.5-hour (Highly recommended) Pre-requisite "HIPAA 101" webinar. (BootCamp Registrants are automatically enrolled.)
II. May 3, 10 & 17, 2018 - Three 3-hour sessions, comprising ten (10) modules, delivered over three weeks (Zoom™ platform)

Attendees will be requested and expected to:

- Engage in live polls conducted in each session
- Post questions and comments for BootCamp™ Faculty to address
- Complete an evaluation after each session

Central Time	Instructional Module	Learning Objectives - Attendees Will Be Able To:	Polling Questions	Faculty Member	Supplemental Material (in addition to presentation slides)
Pre-requisite Session, April 24, 2018 11a – 12:30p Central Time					
11:00am – 12:30pm 90 min. **April 24** **Or** **View Recorded Version**	HIPAA 101	• Demonstrate a working knowledge of the fundamentals of the HIPAA regulations • Explain the history of HIPAA and HITECH and what motivated the creation of these regulations • Identify sources of liability other than HIPAA for CEs and BAs • Articulate the types of organizations which have experienced breaches and complaints • Explain to colleagues and management recent statistics related to breaches of PHI • Describe the relationships between the Privacy, Breach Notification and Security Rules		**Bob Chaput**, MA, CISSP, HCISPP, CRISC, CIPP/US **Erin Brisbay McMahon**, JD	• HIPAA Privacy Rule (link) • HIPAA Security Rule (link) • HIPAA Breach Notification Rule (link) • Omnibus Final Rule (link) • Clearwater CE Omnibus ReadinessCheck™ (link) • Clearwater BA Omnibus ReadinessCheck™ (link) • 30-Minute Guide to Hiring the Best Risk Analysis Company (link) • Harnessing the Power of NIST - Your Practical Guide to Effective Information Risk Management (link) • Connecting the Dots Between Cyber Risk and Patient Safety | How Adopting Information Risk Management and PHI Security Strategies Can Help (link)

Central Time	Instructional Module	Learning Objectives - Attendees Will Be Able To:	Polling Questions	Faculty Member	Supplemental Material (in addition to presentation slides)
Session I – Thursday, May 3, 2018, 11a – 2p Central Time					
11:00am – 11:30am 30 min.	1. Welcome, Introductions and Overview – Session I	• Explain the purpose, scope and objectives of the HIPAA and Cyber Risk Management BootCamp™ to Attendees • Highlight Session I Agenda		**Bob Chaput**, MA, CISSP, HCISPP, CRISC, CIPP/US	1-1. Clearwater White Paper: Harnessing the Power of NIST | Your Practical Guide to Effective Information Risk Management 1-2. Clearwater recorded webinar: Harnessing the Power of the NIST | Your Practical Guide to Effective Cyber Risk Management
11:30 am – 12:15 pm 45 min.	2. Setting the Stage	• Define key risk management terms • Show the relationship between various types of risk • Explain the relation between cyber risk and patient safety • Identify roles and responsibilities • Describe three critical building blocks to establish an effective cyber risk management program		**Bob Chaput**, MA, CISSP, HCISPP, CRISC, CIPP/US	2-1. NISTIR 7298 Revision 2 Glossary of Key Information Security Terms 2-2. Framework for Improving Critical Infrastructure Cybersecurity *(NIST Cybersecurity Framework)* 2-3. Guidance on Risk Analysis Requirements under the HIPAA Security Rule 2-4. NIST SP800-39-final Managing Information Security Risk 2-5. NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments 2-6. NIST SP800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach 2-7. NIST SP800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations 2-8. Harnessing the Power of NIST | Your Practical Guide to Effective Information Risk Management 2-9. NIST SP800-115 Technical Guide to Information Security Testing and Assessment 2-10. HHS/OCR FAQ on 3rd Party Certifications
12:15 pm - 1:00 pm 45 min.	3. A Practical Introduction to Security Controls	• Explain how controls fit in to risk management		**Bob Chaput**, MA, CISSP, HCISPP, CRISC, CIPP/US	3-1. NIST SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations 3-2. California Data Breach Report (February

Central Time	Instructional Module	Learning Objectives - Attendees Will Be Able To:	Polling Questions	Faculty Member	Supplemental Material (in addition to presentation slides)
		• Differentiate between asset- and risk-based risk analysis versus and a controls checklist approach • Make the case for adopting the NIST CSF			2016) 3-3. CIS Top 20 Critical Security Controls v7
Break | 1:00 pm - 1:15 pm					
1:15 pm - 1:45 pm 30 min.	4. Overview of the NIST Cybersecurity Framework (CSF)	• Make the case for adopting the NIST CSF • Explain how the NIST CSF harnesses the power of NIST and five international open standards • Change the conversation of cybersecurity and using an understandable tool • Articulate the benefits of the NIST CSF • Describe the NIST CSF components: Core, Tiers, Profiles • Explain what the NIST CSF is not: not a controls checklist, not a process, and not a maturity model • Articulate the seven steps to implement the NIST CSF		**Bob Chaput**, MA, CISSP, HCISPP, CRISC, CIPP/US	4-1. Framework for Improving Critical Infrastructure Cybersecurity *(NIST Cybersecurity Framework)* 4-2. Choosing an Information Risk Management Framework: The Case for the NIST Cybersecurity Framework (CSF) in Healthcare Organizations *(Clearwater White Paper)* 4-3. (Draft) Cybersecurity Framework v1.1 (PDF) without markup 4-4. (Draft) Cybersecurity Framework v1.1 Core (Excel) 4-5. NIST Video: The Cybersecurity Framework 4-6. NIST Video: Cybersecurity Framework Shared 4-7. AEHIS CHIME Comments on NIST Cyber Framework 2017 4-8. HIMSS-Response-NIST-Cybersecurity-Framework 4-9. The Cybersecurity Framework | Implementation Guidance for Federal Agencies 4-10. SP 800-37 Rev. 2 (DRAFT) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (Discussion Draft) 4-11. NIST 12/21/2017 Webcast: Cybersecurity Framework 101 4-12. Slides for 12/21/2017 NIST Webcast: Cybersecurity Framework 101

Central Time	Instructional Module	Learning Objectives - Attendees Will Be Able To:	Polling Questions	Faculty Member	Supplemental Material (in addition to presentation slides)
1:45 pm - 2:00 pm 15 min.	**Session I – Review and Q&A Most Valuable Concepts/Processes/Practices / Evaluation Reminder**				
Session II – May 10, 2018, 11a-2p Central Time					
11:00 am – 11:15 am 15 min.	Welcome, Introductions and Overview – Session II	• Explain the purpose, scope and objectives of the HIPAA and Cyber Risk Management BootCamp™ to Attendees • Highlight Session II Agenda	• What was the most valuable concept /tool / process discussed in Session I?	**Bob Chaput**, MA, CISSP, HCISPP, CRISC, CIPP/US	
11:15 am – 12:00 pm 45 min.	5. The Critical Difference: HIPAA Security Evaluation vs. HIPAA Security Risk Analysis	• Articulate and cite explicit HIPAA Security Rule requirements • Explain Why Security Evaluation is Not a Risk Analysis and vice versa • Explain what OCR looks for in enforcement regarding Security Evaluation and Risk Analysis • Take practical steps to complete Evaluations and Risk Analyses • Explain how Security Evaluations and Risk Analyses fit into a HIPAA Compliance Program	• Has your organization completed a HIPAA Security Non-Technical Evaluation? • Has your organization completed a HIPAA Security Technical Evaluation? • Has Your Organization Completed a bona fide, comprehensive HIPAA Security Risk Analysis?	**Bob Chaput**, MA, CISSP, HCISPP, CRISC, CIPP/US	5-1. Clearwater blog post: "HIPAA Audit Tips – Don't Confuse HIPAA Security Evaluation and Risk Analysis" 5-2. NIST SP800-115 Technical Guide to Information Security Testing and Assessment 5-3. NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments
12:00 pm - 1:00 pm 60 min.	6. Panel Discussion – Medical Device Risk Management	• Understand the challenges of updating medical device software • Identify medical devices which fall under the purview of a HIPAA Risk Analysis • Establish practical compensating controls to protect against new threats or legacy devices		Moderated by: **Rich Curtiss** Panelist: **Dr. Dale Nordenberg,** MD Executive Director of Medical Device Information, Safety	6-1. AAMI TIR57, Principles for medical device security – risk management 6-2. Guidance on Risk Analysis Requirements under the HIPAA Security Rule 6-3. IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities 6-4. ISO 14971 Medical devices — Application of risk management to medical devices

		• New technologies to assist healthcare in medical device discovery and risk management		and Security Consortium (MDISS) **Dan Bowden,** CISO,Sentara Health **Sue Wang,** Technical Lead of the Healthcare Sector Team, National Cybersecurity Center of Excellence (NCCoE)	6-5. FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance 6-6. FDA Postmarket Management of Cybersecurity in Medical Devices 6-7. Framework for Improving Critical Infrastructure Cybersecurity *(NIST Cybersecurity Framework)* 6-8. *THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY* 6-9. NIST SP1800-8, Securing Wireless Infusion Pumps in Healthcare Delivery Organizations - DRAFT
Break | 1:00 pm - 1:15 pm					
1:15 pm – 1:45 pm 30 min.	7. Overview of the NIST Risk Management Process	• Describe the 4-Step NIST Information Risk Management (IRM) Process • Access NIST and other resources to assist CEs, BAs and Subcontractors in Information Risk Management • Explain the essential steps of establishing, operationalizing and maturing an IRM program • Engage with customers and business partners directly on IRM requirements		**Bob Chaput,** MA, CISSP, HCISPP, CRISC, CIPP/US	7-1. Harnessing the Power of NIST | Your Practical Guide to Effective Information Risk Management *(Clearwater White Paper)* 7-2. NIST SP800-39-final_Managing Information Security Risk 7-3. NIST SP800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach 7-4. NIST SP800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations 7-5. Framework for Improving Critical Infrastructure Cybersecurity *(NIST Cybersecurity Framework)*
1:45 pm - 2:00 pm 15 min.	**Session II – Review and Q&A** **Most Valuable Concepts/Processes/Practices / Evaluation Reminder**				

Central Time	Instructional Module	Learning Objectives - Attendees Will Be Able To:	Polling Questions	Faculty Member	Supplemental Material (in addition to presentation slides)
Session III – May 17, 2018 - 11a – 2p Central Time					
11:00 am – 11:10 am 10 min.	Welcome, Introductions and Overview – Session III	• Explain the purpose, scope and objectives of the HIPAA and Cyber Risk Management BootCamp™ to Attendees • Highlight Session III Agenda		**Bob Chaput**, MA, CISSP, HCISPP, CRISC, CIPP/US	
11:10 am – 12:10 pm 60 min.	8. How to Frame Your Risk Management Program / How to Assess Risks	• Identify key assumptions to make in setting one's IRM strategy • Explain and document IRM constraints • Articulate the importance of setting your risk threshold as part of IRM framing • Be positioned to draft your IRM Strategy and Framework Understand regulatory requirements for ongoing risk assessments • Cite the specific regulatory requirements for risk assessment • Explain why risk assessment is a core foundational step • Describe the steps to complete a thorough and accurate risk analysis	• Have you completed an Information Risk Assessment? • Do you have a program for ongoing risk assessment and risk management?	**Bob Chaput** MA, CISSP, HCISPP, CRISC, CIPP/US	8-1. Clearwater White Paper: Harnessing the Power of NIST | Your Practical Guide to Effective Information Risk Management 8-2. NIST SP800-39-final_Managing Information Security Risk 8-3. NIST SP800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations 8-4. Framework for Improving Critical Infrastructure Cybersecurity *(NIST Cybersecurity Framework)* 8-5. Sample - HIPAA Security Risk Analysis FOR Report 8-6. Guidance on Risk Analysis Requirements under the HIPAA Security Rule 8-7. NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments 8-8. NIST SP800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach 8-9. 30-Minute Guide to Hiring The Best Risk Analysis Company | What to Look for in a HIPAA Risk Analysis Company & Solution (scroll down) 8-10. How to Conduct an OCR-Quality Risk Analysis-On Demand (Webinar)

Central Time	Instructional Module	Learning Objectives - Attendees Will Be Able To:	Polling Questions	Faculty Member	Supplemental Material (in addition to presentation slides)
12:10 pm - 1:10 pm 60 min.	9. How to Manage Risks / How to Monitor Your Risk Management Program	• Understand the regulatory requirements and most effective standards for responding to risk • Know the four essential options for effective risk response Evaluate alternatives to reduce risks in terms of effectiveness and Feasibility • Learn how to make sure risk responses get implemented through tracking new or improved controls	• Do all risks require a response?	**Jon Stone, VP, Product Innovation** MPA, PMP, CRISC, HCISPP	9-1. NIST SP800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (link) 9-2. NIST SP800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (link) 9-3. NIST Interagency Report 7756 CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture (Second Draft) 9-4. NIST Interagency Report 7799 Continuous Monitoring Reference Model, Workflow, and Specifications (Draft) 9-5. NIST Interagency Report 7800 Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains (DRAFT) 9-6. Using risk-based Metrics (pdf)
Break | 1:10 – 1:15 pm					
Course Evaluation 1:15-1:20 pm					
1:20 pm - 1:55 pm 35 min.	10. Now what? – Summary and Action Planning	• Identify Immediate Next Actions for Your Organization • Build Your Cyber Security Business Case • Access Resources and Information Provided During BootCamp™	• In what way would Clearwater best be able to assist you?	**Bob Chaput** MA, CISSP, HCISPP, CRISC, CIPP/US **Jon Stone, VP, Product Innovation** MPA, PMP, CRISC, HCISPP	10-1. Connecting the Dots Between Cyber Risk and Patient Safety *(Clearwater White Paper)* 10-2. Hacking Hospitals *(Independent Security Evaluators Research Report)* 10-3. Top 10 Health Technology Hazards for 2016 (*ECRI Institute Report)* 10-4. Information Risk Management Capability Advancement Model *(Clearwater White Paper)*
1:55 pm - 2:00 pm	**Session III - Review and Q&A Most Valuable Concepts / Processes / Practices? Evaluation Reminder**				