InstaMed®
a J.P.Morgan company

Protect Payments at Every Touchpoint With InstaMed

InstaMed is unmatched when it comes to security, compliance and technological infrastructure, to ensure that your healthcare payments process meets the highest levels of security and compliance. InstaMed is independently audited on a daily basis in all aspects of the healthcare and payment industries.

Achieving PCI Compliance with AMSURG and InstaMed

AMSURG

What Do Centers Need to Do?

For more information, contact your AMSURG dedicated support team at InstaMedPCI@amsurg.com to learn how to:

- Complete PCI questionnaire via Control Scan online
- Schedule required, quarterly vulnerability scans of payment environment

INDEPENDENT AUDITS AND CERTIFICATIONS

- PCI
- EHNAC
- SSAE18 SOC 1 and SOC 2 Examination
- CAQH CORE Phase I, Phase II and Phase III
- HITRUST

ACTIVE SECURITY MONITORING

- **TrustWave**
  InstaMed is audited and scanned for PCI compliance by TrustWave, the leading provider of data security and compliance services to all businesses in the payment industry including acquirers, service providers, third-party providers and merchants. This includes regular onsite assessment, monthly vulnerability scans and network penetration testing.

- **McAfee Secure™**
  InstaMed is regularly scanned for vulnerabilities by McAfee SECURE™ and is a member of their HackerSafe® program.

- **Thawte**
  InstaMed uses 128-bit SSL certificates from Th wte to deliver trusted, secure eCommerce connectivity.

- **Internal Monitoring**
  InstaMed uses multiple layers of internal vulnerability management and monitoring.

SYSTEM AVAILABILITY

InstaMed maintains system availability 24 hours a day, 7 days a week and 365 days a year, excluding scheduled maintenance, in which case InstaMed will notify customers in advance. InstaMed records a system availability that exceeds 99.9%.

DATA CENTERS

InstaMed operates state-of-the-art, secure, redundant and geographically dispersed data centers to deliver superior levels of security and reliability. Each data center has numerous built-in backup systems. Data is mirrored and ensures our ability to deliver the highest levels of industry uptime and disaster recovery capabilities.

POINT-TO-POINT ENCRYPTION (P2PE) AND EMV

- **PCI-Validated P2PE v2.0**

InstaMed is the first and only in healthcare to be PCI-Validated for P2PE v2.0. InstaMed offers healthcare organizations the highest level of security for stored and processed payment card data available in the healthcare industry. P2PE (point-to-point encryption) is a methodology for securing credit card data by encrypting it from the time a card is swiped or keyed until it reaches a secure endpoint (InstaMed) where it is decrypted. InstaMed customers that collect card payments with P2PE v2.0 reduce their PCI compliance programs and leverage the highest levels of security and compliance possible.

- **EMV**

InstaMed is certified with all four card brands for contact Europay, MasterCard and Visa (EMV) on the InstaMed Payment Card interface. EMV is a global standard for authenticating credit and debit card transactions with integrated circuit cards, or “chip cards” at capable point of sale (POS) terminals. EMV certification ensure that InstaMed can offer the highest levels of security for processing these chip cards.

DISASTER RECOVERY

InstaMed’s industry leading business continuity and disaster recovery plan has been independently reviewed as part of our PCI Level One certification and our full accreditation by EHNAC. InstaMed’s bi-coastal operations and data centers ensure rapid restoration of business service in the event of major disaster or failure. Data is synchronized in real-time between our fully redundant, state-of-the-art data centers, and personnel on both coasts are trained on disaster recovery procedures. As a result of our planning and cutover protocols, customers would resume normal operations across our customer base with a target of one hour Recovery Time Objective (RTO) for real-time transaction processing and 24-hour RTO for all batch transaction processing. In addition, print production can be moved to any one of our six facilities in case of a disruption in service.

This material was prepared exclusively for the benefit and internal use of the JPMC client or prospect to whom it is directly addressed (including such entity's subsidiaries, the "Company") in order to assist the Company in evaluating a possible transaction(s) and does not carry any right of disclosure to any other party. In preparing these materials, we have relied upon and assumed, without independent verification, the accuracy and completeness of all information available from public sources or which was provided to us by or on behalf of the Company or which was otherwise reviewed by us. This material is for discussion purposes only and is incomplete without reference to the other briefings provided by JPMC. Neither this material nor any of its contents may be disclosed or used for any other purpose without the prior written consent of JPMC.

J.P. Morgan, JPMorgan, JPMorgan Chase, Chase and InstaMed are marketing names for certain businesses of JPMorgan Chase & Co. and its subsidiaries worldwide (collectively, "JPMC"). Products or services may be marketed and/or provided by commercial banks such as JPMorgan Chase Bank, N.A., securities or other non-banking affiliates or other JPMC entities. JPMC contact persons may be employees or officers of any of the foregoing entities and the terms "J.P. Morgan", "JPMorgan", "JPMorgan Chase" "Chase" and "InstaMed" if and as used herein include as applicable all such employees or officers and/or entities irrespective of marketing name(s) used. Nothing in this material is a solicitation by JPMC of any product or service which would be unlawful under applicable laws or regulations.

Investments or strategies discussed herein may not be suitable for all investors. Neither JPMC nor any of its directors, officers, employees or agents shall incur in any responsibility or liability whatsoever to the Company or any other party with respect to the contents of any matters referred herein, or discussed as a result of, this material. This material is not intended to provide, and should not be relied on for, accounting, legal or tax advice or investment recommendations. Please consult your own tax, legal, accounting or investment advisor concerning such matters.

Not all products and services are available in all geographic areas. Eligibility for particular products and services is subject to final determination by JPMC and or its affiliates/subsidiaries. This material does not constitute a commitment by any JPMC entity to extend or arrange credit or to provide any other products or services and JPMC reserves the right to withdraw at any time. All services are subject to applicable laws, regulations, and applicable approvals and notifications. The Company should examine the specific restrictions and limitations under the laws of its own jurisdiction that may be applicable to the Company due to its nature or to the products and services referred herein.

Notwithstanding anything to the contrary, the statements in this material are not intended to be legally binding. Any products, services, terms or other matters described herein (other than in respect of confidentiality) are subject to the terms of separate legally binding documentation and/or are subject to change without notice.

JPMorgan Chase Bank, N.A. Member FDIC.