HIPAA Analytics, LLC
HIPAA Privacy and Security Consulting

HIPAA Privacy and Security Risk Analysis
Auditors Report and Attestation

Prepared for: Vigilant Medical, Inc.
Date: March 30, 2018

March 30, 2018

To: Santosh Venkatesha
Chief Executive Officer
Vigilant Medical, Inc.
1501 St. Paul Street, Suite 123,
Baltimore, MD 21202

Re: HIPAA Attestation of Vigilant Medical, Inc. HIPAA Privacy and Security Controls and Operational Effectiveness as of March 30, 2018.

Dear Mr. Venkatesha,

HIPAA Analytics, LLC has examined the accompanying areas of audit emphasis of Vigilant Medical, Inc. (Vigilant Medical) HIPAA privacy and security controls as it relates to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) standards, specific to a HIPAA Business Associate. Our examination, referred to as a HIPAA Risk Analysis, included procedures to obtain reasonable assurance about whether, Vigilant Medical HIPAA privacy and security controls throughout the specified period, are suitably designed and operational to achieve the control objectives applicable to Vigilant Medical operation that -

1. The accompanying areas of audit emphasis (HIPAA standards relating to a Business Associate) presents fairly, and in all material respects, the aspects of Vigilant Medical policies, procedures and operations.
2. That HIPAA policies and procedures included in the areas of audit emphasis were suitably designed and operational to achieve the control objectives specified in the HIPAA standards.

Our examination was performed applying the HIPAA Administrative Simplification, Regulation Text, 45 CFR 160,162 and 164 Unofficial Version as amended through February 16, 2006, and the final rule (the “Final Omnibus Rule” or “Final Rule”), published on January 17, 2013, by the Office for Civil Rights (“OCR”), and the U.S. Department of Health and Human Services (“HHS”), making changes to the privacy, security and enforcement regulations promulgated under the Administrative Simplification provisions of HIPAA.

We considered Risk Analysis guidance by HHS, OCR Audit Program Protocol and guidance from the National Institute of Standards and Technology (NIST), Special Publication 800-66, Revision 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, and NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012 to those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion. This 800-66, Revision 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, and NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012 to those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our

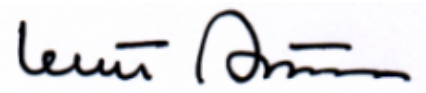
opinion. This report includes HIPAA privacy and security standards relating to Vigilant Medical, Inc. and does not extend to vendors of Vigilant Medical, Inc.

In our opinion, the accompanying areas of audit emphasis (HIPAA privacy and security standards) presents fairly, and in all material respects, the aspects of Vigilant Medical, Inc. policies, procedures and operations. Also, in our opinion, the controls, as described, are suitably designed and operational to provide reasonable assurance to achieve the control objectives specified in the HIPAA privacy and security standards.

The results of design effectiveness of HIPAA policies and procedures at Vigilant Medical, Inc. are as of March 30, 2018. Any projection of such information to the future is subject to the risk that, because of change, the areas of audit emphasis or controls may no longer portray the compliance program currently in existence. The potential effectiveness of specific policies and procedures at Vigilant Medical, Inc. is subject to inherent limitations resulting from non-compliance. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the compliance program or policies and procedures, (2) changes in implementation of policies and procedures, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by management of Vigilant Medical, Inc.

Very truly yours,



Grant Peterson, J.D.
Independent Auditor and Principal
HIPAA Analytics, LLC

EXECUTIVE SUMMARY

Vigilant Medical, Inc. is a medical technology company providing a web application specializing in cloud imaging software, called ImageShare. ImageShare helps physicians review patient images and offer consultations anytime, anywhere in the world.

As a Business Associate within the meaning of HIPAA, Vigilant Medical must comply with the HIPAA Security Standards, certain Privacy Standards and Data Breach regulations in order to ensure the confidentiality, integrity, and availability of all protected health information (PHI) and electronic protected health information (EPHI) that Vigilant Medical creates, receives, maintains or transmits on behalf of a healthcare Covered Entity.

Vigilant Medical, Inc. has requested HIPAA Analytics conduct a HIPAA risk analysis to validate that Vigilant Medical, Inc. HIPAA privacy and security controls are suitably designed and operational to achieve the control objectives as they relate to a HIPAA Business Associate.

On March 14, 2018, Vigilant Medical, Inc. engaged HIPAA Analytics, LLC, to examine the compliance controls in place as it relates to Vigilant Medical, Inc. HIPAA privacy and security standards as to whether -

1. The accompanying areas of audit emphasis (HIPAA standards relating to a HIPAA Business Associate) presents fairly, and in all material respects, the aspects of Vigilant Medical, Inc. policies, procedures and operations.
2. That HIPAA policies and procedures included in the areas of audit emphasis were suitably designed and operational to achieve the control objectives specified in the HIPAA standards.

The risk analysis was conducted using the desk audit method to evaluate Vigilant's state of HIPAA privacy and security compliance. The desk audit requires documentation from Vigilant including; privacy, security and data breach policies and procedures, previous risk analysis reports, data breach and security incident review, contingency plan, PHI and EPHI technical overview, network topology, and management of ImageShare, Business Associate/subcontractor agreements, training, and compliance forms and logs.

In addition, our examination was performed applying the HIPAA Administrative Simplification, Regulation Text, 45 CFR 160,162 and 164 Unofficial Version as amended through February 16, 2006, and the final rule (the "Final Omnibus Rule" or "Final Rule"), published on January 17, 2013, by the Office for Civil Rights ("OCR"), and the U.S. Department of Health and Human Services ("HHS"), making changes to the privacy, security and enforcement regulations promulgated under the Administrative Simplification provisions of HIPAA.

Our examination was performed applying Risk Analysis methods adopted by HHS and OCR Audit Program Protocol and NIST, Special Publication 800-66, Revision 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012, and applying those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion. This report includes HIPAA privacy and security standards relating to Vigilant Medical, Inc. and does not extend to vendors of Vigilant Medical, Inc. The privacy and security standards objectives were specified by Vigilant Medical, Inc.

About the Health Insurance Portability and Accountability Act (HIPAA)
In 1996, Congress enacted the HIPAA, of which the Administrative Simplification provisions promote efficiency in the healthcare industry through the use of transaction standards for the exchange of health information, privacy standards, and security standards for the use and disclosure of individually identifiable health information. HHS issued the Privacy Rule and Security Rules found within HIPAA establishing a set of national standards for the protection of identifiable health information and safeguarding of electronic protected health information.

HIPAA Privacy Rule
The Privacy Rule standards address the use and disclosure of individuals' health information, called "Protected Health Information" (PHI) by organizations subject to the Privacy Rule, referred to as "Covered Entities," and "Business Associates". The standards provide individuals privacy rights and control how their health information is used.

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the healthcare marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed.

HIPAA Security Rule
The HIPAA Security Rule specifically focuses on the safeguarding of electronic Protected Health Information (EPHI). All HIPAA Covered Entities and Business Associates must comply with the Security Rule, which specifically focuses on protecting the confidentiality, integrity, and availability of EPHI, as defined in the Security Rule. The EPHI that a Covered Entity or Business Associate creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures.

HITECH Act
On February 17, 2009, the American Recovery and Reinvestment Act of 2009 ("ARRA") was signed into law. The ARRA includes the HITECH Act, which contains numerous provisions that significantly expand the scope of the security and privacy rules under HIPAA. Collectively, these

provisions brought about sweeping changes in the way Covered Entities and Business Associates maintain, use and disclose PHI.

HIPAA (Omnibus) Final Rule
On January 17, 2013, OCR and HHS, released the final rule (the "Final Omnibus Rule" or "Final Rule") making certain modifications to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules to improve their workability and effectiveness and to increase flexibility for and decrease burden on the regulated entities. The Final Rule became effective March 26, 2013, and Covered Entities (i.e., health plans, health care providers and health care clearinghouses) and Business Associates generally had 180 days (i.e., September 23, 2013) to comply with the new requirements. This audit relates only to the Privacy, Security, Breach Notification, and Enforcement Rules of HIPAA noted above.

Audit Emphasis: HIPAA Privacy Controls
The Privacy Rule allows Covered Entities (Healthcare providers) and health plans to disclose protected health information to "Business Associates" if the providers or plans obtain satisfactory assurances that the Business Associate will use the information only for the purposes for which it was engaged by the Covered Entity, will safeguard the information from misuse, and will help the Covered Entity comply with certain of the Covered Entity's duties under the Privacy Rule. Covered entities may disclose protected health information to an entity in its role as a Business Associate only to help the Covered Entity carry out its health care functions – not for the Business Associate's independent use or purposes, except as needed for the proper management and administration of the Business Associate.

The Privacy Rule requires that a Covered Entity obtain satisfactory assurances from its Business Associate that the Business Associate will appropriately safeguard PHI it creates, receives, maintains, or transmits on behalf of the Covered Entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the Covered Entity and the Business Associate. Because not all HIPAA privacy policies apply to the Business Associate, Vigilant Medical, Inc. has compiled a comprehensive set of HIPAA privacy policies and "Activated" those policies which impact general safeguarding of PHI or may be additional responsibilities outlined in a Business Associate agreement signed with a Covered Entity. In addition, Vigilant Medical, Inc. has "Reserved" certain privacy policies that may be required in future obligations of a Business Associate agreement or required by law.

Vigilant Medical, Inc. has created internal privacy compliance controls designed to provide reasonable assurance that the organization has complied with HIPAA standards. The internal control system is comprised of a HIPAA compliance program, including policies, procedures and training. Our examination included procedures to obtain reasonable assurance as to whether -

1. The accompanying areas of audit emphasis (HIPAA privacy standards) presents fairly, in all material respects, the aspects of Vigilant Medical, Inc. policies, procedures and controls that may be relevant to a user organization's privacy as it relates to HIPAA.

2. That HIPAA privacy policies and procedures included in the areas of audit emphasis were suitably designed to achieve the control objectives specified in the compliance program, if those policies and procedures were complied with satisfactorily.

In our opinion, the accompanying areas of audit emphasis (HIPAA privacy standards) presents fairly, and in all material respects, the aspects of Vigilant Medical, Inc. policies, procedures and operations. Also, in our opinion, the controls, as described, are suitably designed and operational to provide reasonable assurance to achieve the control objectives specified in the HIPAA privacy standards.

Privacy Standard	Section	Control Objectives
General Privacy Standard [Activated]	§ 164.530 (i)(1)	☑ Suitably Designed and Operational
Minimum Necessary Data [Activated]	§ 164.502 (b)	☑ Suitably Designed and Operational
Verification [Activated]	§ 164.514 (n)	☑ Suitably Designed and Operational
Waiver of Rights Not Allowed [Activated]	§ 164.530 (h)	☑ Suitably Designed and Operational
Documentation [Activated]	§ 164.530 (i)	☑ Suitably Designed and Operational
De-identified Information [Activated]	§ 164.514	☑ Suitably Designed and Operational
Designate Privacy Official [Activated]	§ 164.530 (a)	☑ Suitably Designed and Operational
Train Workforce [Activated]	§ 164.530 (b)	☑ Suitably Designed and Operational
Workforce Sanctions for Non-Compliance [Activated]	§ 164.530 (d)	☑ Suitably Designed and Operational
Business Associate and Subcontractor Agreements [Activated]	§ 164.308(b)(1); § 164.502(e); § 164.504(e); § 164.314(a)(2)(i);	☑ Suitably Designed and Operational
Safeguards – Administrative, Physical, and Technical [Activated]	§ 164.530 (c)	☑ Suitably Designed and Operational
Complaints – Internal [Activated]	§ 164.530 (d)	☑ Suitably Designed and Operational
Patient Complaint Policy [Activated]	§ 164.530(d), § 160.306	☑ Suitably Designed and Operational

Audit Emphasis: HIPAA Security Controls
The HIPAA Security rule adopts national standards for safeguards to protect the confidentiality, integrity, and availability of EPHI.

Confidentiality is designed to assure that data or information is not made available or disclosed to unauthorized persons or processes. Integrity is the function designed to assure that data or information has not been altered or destroyed in an unauthorized manner. Availability is the function that assures that data or information is accessible and usable upon demand by an authorized person. However, under HIPAA, the determination of the specific mechanisms and the specific security features to be implemented remains a business decision in many cases.

Comprehensive, Scalable, Technology Neutral
The security standard is based on three basic HIPAA concepts. First, the standard is comprehensive and coordinated to address all aspects of security. Second, it is scalable, so that it can be effectively implemented by Covered Entities and Business Associates of all types and sizes. Third, it is not linked to specific technologies, allowing Covered Entities and Business Associates to make use of future technology advancements.

Administrative, Physical and Technical safeguards
The security standards define the administrative, physical, and technical safeguards required to protect electronic protected health information. The standards also require Covered Entities and Business Associates to implement safeguards to protect EPHI from unauthorized access, alteration, deletion, and transmission.

The Privacy Rule, by contrast, sets standards for how PHI should be controlled by setting forth what uses, and disclosures are authorized or required and what rights patients have with respect to their health information.

The security standard sets a baseline, or minimum level, of security measures that must be taken by a Covered Entity and Business Associates and stipulates that a Business Associate must also implement reasonable and appropriate safeguards, through a Business Associate Agreement.

Required or Addressable
Within the Security Rule sections, many of the standards contain implementation specifications. An implementation specification is a more detailed description of the method or approach Covered Entities and Business Associates can use to meet a particular standard. Implementation specifications are either “required” or “addressable”. A required implementation specification is similar to a standard, in that a Covered Entity and/or Business Associate must comply with it. Specifications that are addressable require Covered Entities and Business Associates to perform an assessment in order to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the Covered Entity and/or Business Associate environment.

Vigilant Medical, Inc. has created internal security compliance controls designed to provide reasonable assurance that the organization has complied with HIPAA standards. Our examination included procedures to obtain reasonable assurance as to whether –

1. The accompanying areas of audit emphasis (HIPAA security standards) presents fairly, in all material respects, the aspects of Vigilant Medical, Inc. policies, procedures and controls that may be relevant to a user organization's security as it relates to HIPAA.
2. That HIPAA policies and procedures included in the areas of audit emphasis were suitably designed to achieve the control objectives specified in the compliance program, if those policies and procedures were complied with satisfactorily.

In our opinion, the accompanying areas of audit emphasis (HIPAA security standards) presents fairly, and in all material respects, the aspects of Vigilant Medical, Inc. policies, procedures and operations. Also, in our opinion, the controls, as described, are suitably designed and operational to provide reasonable assurance to achieve the control objectives specified in the HIPAA security standards.

Security Standard	**Implementation Specifications (R)=Required, (A)= Addressable**	**Control Objectives**
Security Management process § 164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)	☑ Suitably Designed and Operational
Workforce Security § 164.308(a)(3)	Authorization and/or Supervision (A) Workforce Clearance Procedure Termination Procedures (A)	☑ Suitably Designed and Operational
Assigned Security Responsibility § 164.308(a)(2)	(R)	☑ Suitably Designed and Operational
Information Access Management § 164.308(a)(4)	Access Authorization (A) Access establishment and modification (A)	☑ Suitably Designed and Operational
Security Awareness § 164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-In Monitoring (A) Password Management (A)	☑ Suitably Designed and Operational
Security Incident Procedures § 164.308(a)(6	Response and Reporting (R)	☑ Suitably Designed and Operational
Contingency Plan § 164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)	☑ Suitably Designed and Operational

Evaluation § 164.308(a)(8)	(R)	☑ Suitably Designed and Operational
Business Associate Contracts and Other Arrangement § 164.314(a)(1)	Written Contract or Other Arrangement (R) Subcontractor Agreement	☑ Suitably Designed and Operational
Facility Access Controls § 164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)	☑ Suitably Designed and Operational
Workstation Use § 164.310(b)	(R)	☑ Suitably Designed and Operational
Workstation Security § 164.310(c)	(R)	☑ Suitably Designed and Operational
Device and Media Controls §164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)	☑ Suitably Designed and Operational
Access Control §164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)	☑ Suitably Designed and Operational
Audit Controls § 164.312(b)	(R)	☑ Suitably Designed and Operational
Integrity § 164.312(c)(1)		☑ Suitably Designed and Operational
Mechanism to Authenticate Electronic Protected Health Information § 164.312(c)(2)	(A)	☑ Suitably Designed and Operational
Person or Entity Authentication § 164.312(d)	(R)	☑ Suitably Designed and Operational
Transmission Security §164.312(e)(1)	(A)	☑ Suitably Designed and Operational
Integrity Controls (A) § 164.312(e)(2)(i)		☑ Suitably Designed and Operational
Encryption (A) § 164.312(e)(2)(ii)		☑ Suitably Designed and Operational
Business Associate Contracts and Other Arrangement § 164.314(a)(1)	Written Contract or Other Arrangement (R)	☑ Suitably Designed and Operational

Documentation § 164.316	Policies and Procedures Time Limit Availability(R) Updates(R)	☑ Suitably Designed and Operational
Data Breach Notification § 164.402	Breach Unsecured Protected Health Information	☑ Suitably Designed and Operational