LifeOmic Health Information Protection & HIPAA Compliance

# Executive Statement and Attestation

July 10, 2017

**LifeOmic has implemented a "zero trust" security model with virtually air-gapped and immutable production environments.** An in-depth review of company's information security program, technology and operational infrastructure was performed to assess the program's capability and maturity.

**The result of this assessment certifies that LifeOmic meets and exceeds all areas of HIPAA/HITECH regulations and requirements.** This includes:

## HIPAA Administrative Safeguards

- LifeOmic's CISO is assigned and fully accountable to the HIPAA security and privacy program
- Annual risk assessment has been conducted
- All employees have been through rigorous background checks
- All employees are required to take annual HIPAA awareness and monthly security awareness training
- Formal information security policies and procedures have been implemented
- Business Associate Agreements (BAAs) are executed with all partners who handle protected health information (PHI) or electronic PHI (ePHI)

## HIPAA Technical Safeguards

- Unique user identification is required and tracked for each individual user with access to ePHI
- An emergency access and response plan is established
- Inactive sessions to access ePHI automatically terminate / log off
- Any internal access to ePHI requires strong passwords and second factor authentication
- Access is granted with least-privilege and terminated when no longer needed
- All access to ePHI is monitored and logged
- ePHI is de-identified both in storage and in transit using strong encryption
- ePHI is stored in secure ransomware-proof repositories and replicated across geographical regions

## HIPAA Physical Safeguards

- Physical access to PHI or systems and devices that contain ePHI is controlled by two layers of key cards
- Video security cameras are put in place for 24x7 monitoring
- All physical media containing ePHI are encrypted with strong cryptographic algorithm at device level
- Media is securely wiped or physically destroyed, and encryption keys destroyed prior to reuse or disposal

LifeOmic's information security and data protection program will continue to evolve and improve. We strive to provide the latest innovation in security technology and best practices, to always stay ahead of the threats and protect our customers.

Donald E Brown
Dr. Donald E. Brown
Chief Executive Officer
LifeOmic, Inc.

Erkang Zheng
Digitally signed
by Erkang Zheng
Date: 2017.07.13
09:21:46 -04'00'
Erkang Zheng
Chief Information Security Officer
LifeOmic, Inc.

LifeOmic