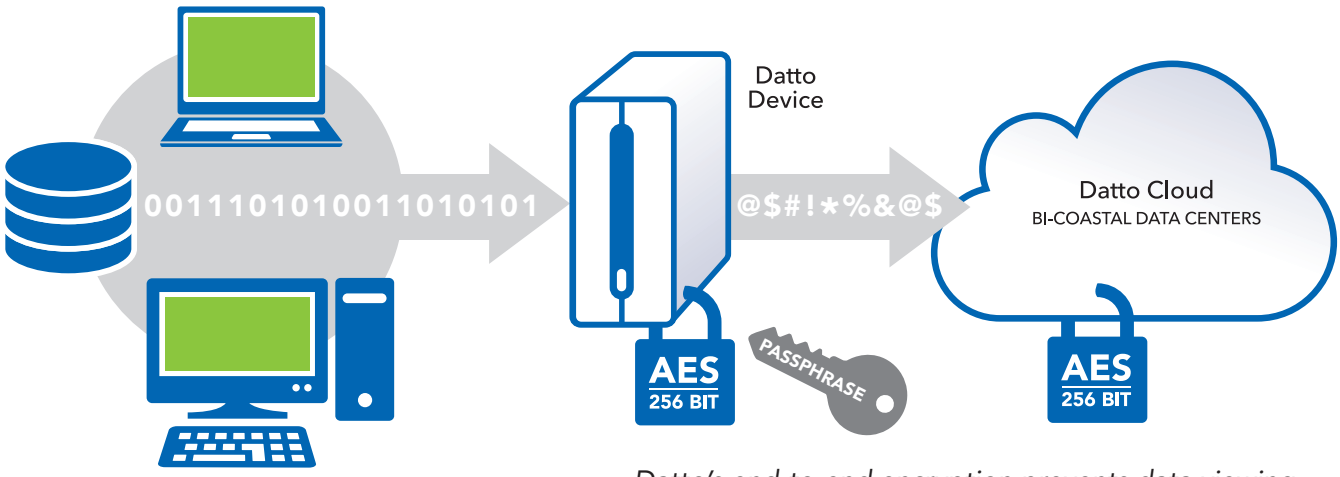
5 Cornerstones of Compliance

DATTO'S INFORMATION SECURITY CONTROLS

by Feisal Nanji, Datto Chief Security Officer



Datto's end-to-end encryption prevents data viewing, tampering or theft during the entire continuity process

For backup and disaster recovery (BDR) solution providers Security Compliance can be a multi-tiered, multi-faceted monster. Industry verticals such as banking, health care, insurance and energy production all have different regulatory requirements to protect information systems.

Adding to this confusion are a bevy of security control frameworks offered by organizations such as the Information Systems Audit and Control Association (ISACA), National Institute of Standards and Technology (NIST) and the International Standards Organization (ISO). Therefore, navigating through this compliance thicket can be confusing if not daunting to Managed Service Providers (MSPs), IT solution providers and even the IT vendors serving the channel.

At Datto, our commitment to providing secure solutions for our Channel Partners is a priority. We also understand that MSPs have varying relationships with their end-user clients; the variables could be the level of support and integration offered to an end-user or a focus on a specific industry vertical. As such, we have designed our security strategy to meet a diverse set of MSP needs. By implication, this means that both the security of our client data and that resident in our own internal systems must reflect this commitment.

This whitepaper takes a look at the five cornerstones of Datto's fundamental approach to compliance:

1. Use a globally accepted controls framework to manage the information security function at Datto
2. Hone in on and meet the most stringent regulatory requirements found across industry verticals
3. Meet all the major regulatory regimes necessary for our Channel Partners to succeed
4. Tailor solutions to meet any international or country specific requirements
5. Demonstrate that the security of Datto's hybrid cloud-based solutions and services are without parallel

1. Datto's Controls Framework

For any entity of significant size, such as Datto, the lack of an information security management system (ISMS), results in controls that tend to be somewhat disorganized and disjointed. Without an ISMS, controls are usually implemented as point solutions to specific situations or simply as a matter of convention.

To achieve the highest level of information security, Datto has adopted the International Standards Organization (ISO) 27000 series of security standards as its ISMS. The ISO 27000 series of security standards is an ISMS standard published by ISO and the International Electrotechnical Commission (IEC).

Datto's adoption of the ISO 27001 standard requires that its management:

- Systematically examine the organization's information security risks, taking into account the threats, vulnerabilities, and impacts
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

The key benefits for Datto's adoption of ISO 27001, and, by extension, for its Channel Partners are:

- It can act as an extension of Datto's current quality system to include security
- It provides an opportunity to identify and manage risks to key information and systems assets
- It allows an independent review and assurance of our information security practices
- It is suitable for protecting critical and sensitive information
- It provides a holistic, risk-based approach to secure information and compliance
- It demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers
- It demonstrates security status according to internationally accepted criteria

2. Datto's Design for Meeting Security Compliance

The 2013 passage of the HIPAA Omnibus rule for health care providers imposes among the strictest control requirements for health care delivery providers and its vendor base. Among the new changes, "Business Associates" (solution vendors such as Datto) must comply with security and breach notification rules. By abiding to HIPAA requirements Datto, in essence, has voluntary applied to itself among the most stringent security requirements.

To elaborate, under HIPAA, all Business Associates who will have access to unencrypted electronic protected health information (ePHI) for technical support or administrative reasons are required to comply with HIPAA. As a backup and disaster recovery solution vendor, Datto does have such access and so Datto is, de-facto, a Business Associate to end-users that are Covered Entities. Datto must therefore secure ePHI using a prescribed controls framework that provides adequate safeguards for physical facilities, administrative requirements (e.g. adequate security policies) and technical infrastructure.

Specifically, Business Associates must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance by their workforce

The 2013 additions to the HIPAA Omnibus rule also specifically define cloud service providers (CSPs) as Business Associates: '*...document storage companies maintaining protected health information on behalf of covered entities are considered Business Associates, regardless of whether they actually view the information they hold.*' Thus, MSPs (IT Solution Providers, Value Added Resellers (VARs) and the like) of cloud based services and products are also "Business Associates" and must achieve HIPAA compliance.

To ensure that Datto meets the full intent of compliance under HIPAA, Datto conducts an annual security risk analysis process to include the following activities:

- Evaluate the likelihood and impact of potential risks to ePHI
- Implement appropriate security measures to address the risks identified in the risk analysis
- Document the chosen security measures and, where required, the rationale for adopting those measures
- Maintain continuous, reasonable, and appropriate security protections

HIPAA Regulatory Considerations for Datto MSPs and VARs

For Datto's Channel Partners implementing a full set of such controls can be complicated and expensive. However the law absolves MSPs and VARs from risk due to any data breach if the health data handled is adequately encrypted. This is known as the "Safe Harbor Provision." The specific reading under the law is: *"Secured protected health information means protected health information that is rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5".*

In essence, a storage solution that adequately prevents an MSP or VAR from inadvertently or intentionally looking at ePHI (thus constituting a breach) provides a "Safe Harbor" or "get out of jail free" card. If an MSP uses Datto's forthcoming end-end encrypted solutions—from Health Care provider right through to Datto's Cloud and data centers—the MSP can achieve Safe Harbor and meet HIPAA requirements without having to conduct exhaustive compliance programs of their own.

We caution, however, that if MSPs or VARs handle or have access to unencrypted ePHI they must also abide by HIPAA requirements. Part of the requirements include conducting an annual security risk assessment and developing a risk management plan. We recommend that each MSP develop an ongoing process where it reviews its records to track access to Covered Entity ePHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to ePHI. For MSPs seeking direction on how to do this, Datto has dedicated resources to assist MSPs.

3. Regulatory Regime Coverage

Datto has set the HIPAA security requirements as its minimum baseline. The use of HIPAA as a baseline more than meets requirements for most all industries. Additional control measures, if warranted by other more stringent industries e.g. Nuclear Power Plants, will be adopted by Datto when required.

Datto will also abide by requirements put forth by the Payment Card Industry—Data Security Standard 2.0 (PCI-DSS 2.0), and any successive additions to this set of compliance requirements, as well as any banking and finance regulations such as the Gramm Leach Bliley Act (GLBA), and the Federal Rules for Civil Procedure (FRCP).

4. Geographical and International Tailoring

Various states and countries, and industries within them, have different requirements or regulations for handling data. To ensure that Datto's international efforts remain unimpeded, Datto will constantly analyze and adhere to such requirements.

For example, the backup and data storage locations for Datto's cloud operations must meet certain US export restrictions. To elaborate, the transmission of data to a cloud platform for manipulation or storage is not conceptually different for export control purposes than carrying

a hard copy of that data abroad or sending it through the mail. Transmission of data to the cloud for processing or backup involves copying that data to a server or group of servers. If the location of the cloud is outside the U.S., then sending the data to the cloud server for processing or storage is an export. If the data or software sent to the cloud server is export controlled, then doing so is an export of controlled technical data as surely as if it had been copied on paper and carried abroad.

Examples of internationally focused regulations Datto has to meet include:

- Export Administration Regulations ("EAR") administered by the Department of Commerce
- The International Traffic in Arms Regulation ("ITAR") administered by the Department of State
- Economic and trade sanctions rules administered by the Treasury's Office of Foreign Assets Controls ("OFAC")
- The European Data Protection Directive
- Canada's two federal privacy laws, the Privacy Act and the Personal Information Protection and Electronic Documents Act

5. Datto's Efforts to Create "Regulatory Safe" Solutions and Products

Among the initiatives Datto aims to provide to reduce compliance burdens on MSPs, VARs and their respective end-user clients are:

- Provision of **end-to-end encryption data storage services** that prevents data viewing, tampering or theft during storage once it leaves the premises or infrastructure of the End User (see the diagram on page 1).
    - ❯ One option to achieve this is the way Datto handles encryption "keys" for certain industries e.g. health care. Here, Datto's designs can insist that end-users alone and not MSPs and VARs will ever have access to encryption keys to decrypt any data.
- **Data integrity checking** to ensure that data has not been tampered with during transit.
- Backup capabilities that allow end-users to **fully expect** any data is always backed up and retrievable within a prescribed window.
    - ❯ This is a key requirement for Business Associates and Covered Entities who can use this guarantee to demonstrate HIPAA compliance requirements for backup, data recovery and emergency mode operation, and contingency plans.
- **Advanced logging and monitoring features,** that can display who may have viewed, edited or added any unencrypted data to Datto appliances. Managers of the Datto Cloud who may have access to unencrypted data for the purposes of data management will also be identified and logged.
    - ❯ For Health Care providers this set of management features is instrumental in meeting access control, and logging and monitoring requirements under HIPAA.

- Datto Cloud centers and services will have the appropriate set of required **physical, administrative and technical controls** to ensure that no breach shall occur by Datto as part of its data handling process.
- Procedure for securely destroying any customer Covered Entity data upon termination of a contract, or when swapping out hardware.
- For U.S.-based customers, provide U.S.-based Datto service and support personnel, and to keep all data within U.S. borders

Summary

At Datto, we have designed our security strategy to meet the diverse needs of all our Channel Partners. By implication this means that both the security of our client data and that resident in our own internal systems must reflect this commitment.

Additional resources you may find useful in navigating the domain of Compliance are:

- **The Datto Compliance 101 booklet** provides an overview of the HIPAA compliance requirements for MSPs and VARs. It covers relevant legislation, required procedures, risk assessment, and ways that your business can achieve compliance. http://dattobackup.com/compliance-guidebook
- **Webinar on HIPAA compliance regulations.** Watch this informative Webinar with Datto's Chief Security Officer Feisal Nanji, Director of Product Ian McChord, and MSPmentor's Joe Panettieri. http://dattobackup.com/hipaa-compliance-with-datto

About Datto

Datto Inc. is an award-winning vendor of backup, disaster recovery (BDR) and Intelligent Business Continuity (IBC) solutions, providing best-in-class technology and support to its 5,000+ channel Partners throughout North America and Europe. Datto is the only hybrid-cloud BDR/IBC vendor that provides instant on- and off-site virtualization, and screenshot backup verification, achieved through its Inverse Chain Technology.™

The Datto product line addresses the specific needs of small to medium-sized businesses (SMBs). The product line is comprised of Datto SIRIS, Datto SIRIS Lite, Datto ALTO, Datto G Series, and Datto GenISIS. Its solutions serve a wide range of vertical markets including: healthcare, financial, education, banking, legal, manufacturing, retail, and municipal.

Datto partners with the best technology providers in the industry to deliver the most robust and seamless BDR and business continuity solutions available, including: AutoTask, ConnectWise, Kaseya, Level Platforms and StorageCraft.

Founded in 2007 by Austin McChord, Datto is privately held.

Datto, Inc.
101 Merritt 7
Norwalk, CT 06851
partners@dattobackup.com

USA: 888.294.6312
Canada: 877.811.0577
UK: (01224) 451475