Compliance – A primer

Surveys indicate that 80% of the spend on IT security technology is driven by the need to comply with regulatory legislation.

The growth in the sharing of sensitive data combined with the increased use of computing technology has fuelled concerns over the security, integrity and ownership of sensitive data.

These concerns have led to the rise of many regulatory bodies around the world. Some bodies regulate specific industry sectors (HIPAA), some regulate specific processes (SOX) and some regulate the general use of data regardless of its specific use (Data Protection Act, Information Commissioner's Office). Regardless of the specific focus of the regulatory bodies they all share similar remits.

- *To recommend the use of best practices for the handling of sensitive data*
- *To safeguard the privacy of sensitive data, in whatever format it exists in*
- *To protect the interests of the "data owner", be they corporate or personal*
- *To penalise organizations that fail to comply with regulations*

Regulatory bodies do not focus solely on data handling in an IT specific world; in fact the only constant in all of the regulations is the data itself. Data can take many formats, electronic, hard copy, verbal, and most compliance standards relate to data in all of these formats. We should not just think of data in just its IT or electronic format.

When explaining how Celestix helps organizations to comply with regulatory compliance we must be very clear on exactly what we do to help the organization. We must not talk in too general terms for the risk of sounding inexperienced or unfamiliar with the core content. We must also be cautious not to oversell our capability in supporting organizations in the drive to comply.

There are many regulatory bodies and it is not practical to reference all of them in this document. Instead we will focus on the three most common and widely understood regulatory codes of conduct. It should be assumed that all regulatory bodies will issue guidelines that are similar in nature to those outlined in this document.

celestix

PCI DSS - Payment Card Industry (PCI) Data Security Standard

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks.

The PCI Security Standards Council (PCI SSC) website (www.pcisecuritystandards.org) contains a number of additional resources

Below is a high-level overview of the 12 PCI DSS requirements.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

The PCI DSS security requirements apply to all system components. In the context of PCI DSS, system components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. System components also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. The cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are

not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (for example, Internet) applications.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know
To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

Requirement 8: Assign a unique ID to each person with computer access
Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.

8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric

8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.)
Note: *Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.*

8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.

8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components

8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.

8.5.2 Verify user identity before performing password resets.

8.5.3 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.

8.5.4 Immediately revoke access for any terminated users.

8.5.5 Remove/disable inactive user accounts at least every 90 days.

8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.

8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data.

8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.

8.5.9 Change user passwords at least every 90 days.

8.5.10 Require a minimum password length of at least seven characters.

8.5.11 Use passwords containing both numeric and alphabetic characters.

8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.

8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.

8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.

8.5.15 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.

Restrict user direct access or queries to databases to database administrators.

10.2.4 Verify invalid logical access attempts are logged.

10.2.5 Verify use of identification and authentication mechanisms is logged.

12.3.2 Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (for example, token).

12.3.3 Verify that the usage policies require a list of all devices and personnel authorized to use the devices.

HIPAA - The Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that specifies administrative simplification provisions that:

- Protect the privacy of patient information
- Provide for electronic and physical security of patient health information
- Require **"minimum necessary"** use and disclosure
- Specify patient rights to approve the access and use of their medical information
- Apply to individuals as well as institutions
- Unauthorized access includes the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment or other lawful use
- Licensed facilities, like UCSF Medical Center, are required to report incidents of unauthorized access, use, or disclosure of PHI to the California Department of Public Health, and to the affected patient within 5 business days after breach detection
- When you suspect or know of a breach you must report it to the Privacy Office **immediately**
    - Medical Center employees must also submit an Incident Report

In addition to HIPAA, there are other federal laws which govern the release of information, mandate that information be protected, and in some cases require that individuals be granted certain rights relative to control of and access of their information.

- **The Medicare Conditions of Participation** require that hospitals promote each patient's rights, including privacy (42 CFR Section 482.13).
- **The Federal Trade Commission (FTC)** charged with protecting consumers requires banking and other industries to implement "red flag" standards (12 CFR Part 681) to detect and prevent identity theft related to customer and service accounts. These red flag rules extend to Health Care Institutions.

- **The Family Education Rights and Privacy Act (FERPA)** governs the protection of education records which include student health records (20 USC 1232g). HIPAA specifically exempts individually identifiable health information in education records. As FERPA records are exempt from HIPAA, all releases from education records must be in accordance with FERPA regulations.
- Federal Department of Health and Human Services (HHS) as well as multiple federal agencies require the protection of the privacy and confidentiality of participants in research clinical trials.

Confidentiality of Medical Information Act (CMIA) (Civil Code Section 56 et seq.) requires that:

- Confidentiality of Medical Information be protected and establishes protections against disclosures of Individually Identifiable Medical Information
- Institutions notify California residents of breaches of electronic social security number, access codes to financial accounts, medical, and insurance information
- Healthcare institutions implement safeguards to protect the privacy and confidentiality of Medical Information

Civil Code Sections 1785.11.2, 1798.29, 1798.82 and Health & Safety Code Section 130200

Health & Safety Code Section 1280.15 mandates that licensed clinics and health facilities report to both the Department of Public Health and the affected patient(s) any unlawful or unauthorized access to, or use or disclosure of, a patient's Medical Information no later than 5 calendar days after the breach is detected.

Lanterman-Petris-Short (LPS) (Welfare and Institutions Code Section 5328 *et seq*.) provides special confidentiality protections for medical records containing mental health or development disabilities information.

Title 22, California Code of Regulations, Section 70707(b)(8), requires acute care hospitals to protect patient rights to the confidential treatment of all information related to their care and stay at the hospital.

- HIPAA Criminal Penalties
  - $50,000 - $1,500,000 fines
  - Imprisonment up to 10 years
- HIPAA Civil Penalties
  - $100 - $25,000 / year fines
  - More fines if multiple year violations
- State Laws
  - Fines and penalties apply to individuals as well as health care providers, up to a maximum of $250,000; may impact your professional license

    - Imprisonment up to 10 years
- UCSF corrective and disciplinary actions
    - Up to and including loss of privileges and termination of employment

Who Uses PHI?

- Anyone who works with or may view health, financial, or confidential information with HIPAA protected health identifiers
- Everyone who uses a computer or electronic device which stores and/or transmits information
- The following workforce members:
    - All Medical Center staff
    - Faculty Group Practice staff
    - Schools of Medicine, Nursing, Dentistry: staff and faculty
    - Campus staff who work in clinical areas
    - Administrative staff with access to PHI
    - Volunteers
    - Students who work with patients
    - Researchers and staff investigators
    - Accounting and payroll staff
    - Almost **EVERYONE,** at one time or another

Examples of Privacy Breaches

- Talking in public areas, talking too loudly, talking to the wrong person
- Lost/stolen or improperly disposed of paper, mail, films, notebooks
- Lost/stolen laptops, PDAs, cell phones, media devices (video and audio recordings)
- Lost/stolen zip disks, CDs, flash drives, memory drives
- Hacking of unprotected computer systems
- Email or faxes sent to the wrong address, wrong person, or wrong number
- User not logging off of computer systems, allowing others to access their computer or system

Computer Security

- Create a strong password and **do not share** your username or password with **anyone**
- Log off your computer terminal when you are done, or even if you walk away for a few moments

A physician is very busy and asks you to log into the clinical information system using his user ID and password to retrieve some patient reports. What should you do?

celestix

1998 Data Protection Act

The data protection act is enforced in the UK by the Information Commissioner's Office (ICO) which can levy penalties of up to $800,000 per data breach on any organization, regardless of vertical sector. Instances of breach are regularly publicised by the ICO and are widely referenceable online and in the press.

The DPA concentrates on data breach pertaining to "personal data" – PHI, account records, educational records etc.

What needs to be protected by information security arrangements?

10. It is important to understand that the requirements of the Data Protection Act go beyond the way information is stored or transmitted. The seventh data protection principle relates to the security of every aspect of your processing of personal data.

11. So the security measures you put in place should seek to ensure that:

- only authorised people can access, alter, disclose or destroy personal data;
- those people only act within the scope of their authority; and
- if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.