Incident Handling and Legal Compliance

Objectives:

At the end of this episode, I will be able to:

Understand what the role of Laws in Incident Handling is, as well as the various legal and jurisdictional issues that an IH&R team member must be aware of when dealing with an incident.

Explain what Incident Handling and legal compliance concerns an IH&R team member needs to be aware of.

Identify the various legal frameworks that an IH&R team member should be familiar with.

Define what key action(s) and area(s) of focus an IH&R team member should associate with the various legal frameworks.

External Resources:

Incident Handling and Legal Compliance

Role of Laws in Incident Handling -

Cyber laws are integral to incident handling as they provide the assurance of the integrity, security, privacy, and confidentiality of information in both government and private organizations.

Cyber laws vary by jurisdiction and country, so implementing these laws is quite challenging.

Violating these laws may result in punishments ranging from fines to imprisonment.

Legal and Jurisdictional Issues when Dealing with an Incident -

An organization can be subjected to different jurisdictions as per the location where it operates.

It is essential for organizations to stay alert about data breach notifications that are reported from each jurisdiction in which they function and have internal policies aligned with applicable laws to deal with such scenarios.

Following are the ways to handle legal and jurisdictional issues when dealing with an incident:

```
▪ Law enforcement agencies should be contacted only through designated
individuals

▪ Organizations should not contact multiple agencies because it might result
in jurisdictional conflicts

▪ Consult lawyers if an illegal act has occurred and if there are reporting
responsibilities
```

Incident Handling and Legal Compliance -

Sarbanes–Oxley Act (SOX) - Enacted in 2002, aims to protect investors and the public by increasing the accuracy and reliability of corporate disclosures. This act does not explain how an organization needs to store records, but describes records that organizations need to store and the duration of the storage.

Key requirements and provisions of SOX are organized into 11 titles:

Title I: Public Company Accounting Oversight Board (PCAOB) - consists of nine sections and establishes the Public Company Accounting Oversight Board to provide independent oversight of public accounting firms providing audit services (“auditors”). It also creates a central oversight board tasked with registering audit services, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

Title II: Auditor Independence - consists of nine sections and establishes standards for external auditor independence to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (for example, consulting) for the same clients.

Title III: Corporate Responsibility - consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction of

external auditors and corporate audit committees and specifies the responsibility of corporate officers for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance.

Title IV: Enhanced Financial Disclosures - consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and stock transactions of corporate officers. It requires internal controls for assuring the accuracy of financial reports and disclosures and mandates both audits and reports on those controls. It also requires timely reporting of material changes in the financial condition and specific enhanced reviews by the Securities and Exchange Commission (SEC) or its agents of corporate reports.

Title V: Analyst Conflicts of Interest - consists of only one section, which includes measures designed to help restore investor confidence in the reporting of securities analysts. It defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.

Title VI: Commission Resources and Authority - consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and conditions to bar a person from practicing as a broker, advisor, or dealer.

Title VII: Studies and Reports - consists of five sections and requires the Comptroller General and the SEC to perform various studies and report their findings. Studies and reports include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations, and enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

Title VIII: Corporate and Criminal Fraud Accountability - also known as the "Corporate and Criminal Fraud Accountability Act of 2002," consists of seven sections. It describes specific criminal penalties for manipulation, destruction, or alteration of financial records or other interference with investigations, while providing certain protections for whistle-blowers.

Title IX: White-Collar Crime Penalty Enhancement - also known as the "White Collar Crime Penalty Enhancement Act of 2002," consists of six sections. This title increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

Title X: Corporate Tax Returns - consists of one section and states that the Chief Executive Officer should sign the company tax return.

Title XI: Corporate Fraud Accountability - consists of seven sections. Section 1101 recommends the following name for this title: "Corporate Fraud Accountability Act of 2002." It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to resort to temporarily freezing "large" or "unusual" transactions or payments.

The Health Insurance Portability and Accountability Act (HIPAA) -

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information.

At the same time, the Privacy Rule permits the disclosure of health information needed for patient care and other important purposes.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

The National Provider Identifier (NPI) is a Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Standard.

The NPI is a unique identification number for covered healthcare providers. Covered healthcare providers and all health plans and healthcare clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA.

The NPI is a ten-position, intelligence-free numeric identifier (ten-digit number). This means that the numbers do not carry other information about healthcare providers, such as the state in which they live or their medical specialty.

Federal Information Security Management Act of 2002 (FISMA) - provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.

It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

The FISMA framework includes:

```
▪ Standards for categorizing information and information systems by mission
impact

▪ Standards for minimum security requirements for information and information
systems

▪ Guidance for selecting appropriate security controls for information systems

▪ Guidance for assessing security controls in information systems and
determining security control effectiveness

▪ Guidance for the security authorization of information systems
```

Gramm–Leach–Bliley Act (GLBA) - requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data.

The objective of the Gramm–Leach–Bliley Act is to ease the transfer of financial information between institutions and banks while making the rights of the individual through security requirements more specific.

Its provisions limit when a “financial institution” may disclose a consumer’s “nonpublic personal information” to nonaffiliated third parties.

The UK Data Protection Act 2018 (DPA), passed on 23 May 2018, is the UK implementation of the EU’s GDPR legislation, codifying its requirements into UK law.

It provides protection of personal data in the following way:

```
o Requiring personal data to be processed lawfully and fairly, on the basis
of the data subject’s consent or another specified basis

o Conferring rights on the data subject to obtain information about the
processing of personal data and to require inaccurate personal data to be
rectified

o Conferring functions on the Commissioner, giving the holder of that office
responsibility for monitoring and enforcing their provisions
```

General Data Protection Regulation (GDPR) - replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizen’s data privacy, and to reshape the way organizations across the region approach data privacy.

Article 32: Technical and organizational measures need to provide:

```
o The ability to ensure the ongoing confidentiality, integrity, availability,
and resilience of processing systems and services

o The ability to restore the availability and access to personal data on time
in the event of a physical or technical incident

o A process for regularly testing, assessing, and evaluating the effectiveness
of technical and organizational measures for ensuring the security of the
processing
```

Article 33(1): In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is

unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The Digital Millennium Copyright Act (DMCA) - a US copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.

It defines legal prohibitions against circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information in order to implement US treaty obligations.

The DMCA contains five titles:

Title I: WIPO TREATY IMPLEMENTATION - implements the WIPO treaties. First, it makes certain technical amendments to US law in order to provide appropriate references and links to the treaties. Second, it creates two new prohibitions in Title 17 of the US Code—one on circumvention of technological measures used by copyright owners to protect their works and one on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions.

Title II: ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION - adds a new section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. A service provider bases the limitations on the following four categories of conduct:

```
o Transitory communications
o System caching
o Storage of information on systems or networks at direction of users
o Information location tools
```

NOTE: New section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

Title III: COMPUTER MAINTENANCE OR REPAIR - allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer.

Title IV: MISCELLANEOUS PROVISIONS - contains six miscellaneous provisions, where the first provision provides Clarification of the Authority of the Copyright Office, the second provision grants exemption for the making of “ephemeral recordings”, the third provision promotes distance education study, the fourth provision provides exemption for Nonprofit Libraries and Archives, the fifth provision allows Webcasting Amendments to the Digital Performance Right in Sound Recordings, and the sixth provision addresses concerns about the ability of writers, directors, and screen actors to obtain residual payments for the exploitation of motion pictures in situations where the producer is no longer able to make these payments.

Title V: PROTECTION OF CERTAIN ORIGINAL DESIGNS - entitles the Vessel Hull Design Protection Act (VHDPA). It creates a new system for protecting original designs of certain useful articles that make the article attractive or distinctive in appearance. For purposes of the VHDPA, “useful articles” are limited to the hulls (including the decks) of vessels no longer than 200 feet.