# Research Paper- Team 08

# **Data Breach Response Policy**

# Hariharan Balakrishnan

# Apoorva Ajith Prasad

Sakshi Yashwant Tayade

Pooja Uradi

Mercy Newncia Kadaviparambil

IFT 598 - Developing Security Policy

Dr. Tatiana Walsh

02/12/2022

**Research Statement**

As a result of a data breach, the organization must develop a data breach response plan that describes what constitutes a cybersecurity issue, who is involved, and what they should do in the event of such an incident.

#### **The Introduction**

Generally, a privacy breach occurs when protected information is used or disclosed unlawfully. The act of copying, transmitting, viewing, taking, or using sensitive, protected, or confidential information constitutes a security violation. An owner is unaware or consent less when information is extracted from their system. A huge organization or a small firm might have a data breach. Credit card numbers, customer information, trade secrets, and national security data are examples of sensitive, proprietary, or private information which may have been stolen. According to the number of data breaches recorded between January 2005 and April 2015, financial data is the second most frequently stolen data type, after personally identifiable information (PII). Unintended exposure to information is another name for data spills, data leaks, and information leakage (Data Breach - Definition, n.d.).

In the case of data breaches, companies may have to spend a lot of money to fix the damage, investigate the incident, and provide cyber protection to the people who were affected by the breach (Data Breach - Definition, n.d.).

**Purpose Of the Policy**

### The methods of data management have switched from using paper records to electronic data systems and web-based apps to store, process, and send any type of data to within the organization internally, externally or to even a third party. These data can contain a significant amount of personally identifiable information (PII) from records that must be managed and secured properly. Data theft, data breaches, and data exposures are handled differently according to the type of data involved (Rd et al., n.d.).

### Establishing and implementing a clear data breach response policy which outlines essential steps and tools for responding to a data breach, is a very important task. This policy provides organizations with tools for the data breach that has already occurred, where some include reporting suspected data theft, data breaches, or data exposures (Rd et al., n.d.).

**Data breach**

A data breach occurs if personally identifiable information (PII) or other data not authorized for public release is released or accessed by an unauthorized party. This concept holds true whether a company stores and manages its data in-house or through a third party, such a cloud service provider (*Data Breach Response*, 2019).

The secured data can be accessed through multiple ways, some if them are mentioned below,

* Malicious attacks by hackers
* The equipment like laptops, mobiles etc., get stolen, misplaced and so on.
* Negligence of the employee by leaving personal information passcodes etc. publicly
* Policy / system failure

**Data breach response policy**

Your company will have a roadmap to follow in the event of a data breach. In order to put together the data breach response plan, a few essential components must be considered. A data breach response plan is a tool you can use to deal with a data breach. An organization should follow this framework in order to manage a data breach in a suitable way, as well as to determine how to respond when a breach occurs (*Data Breach Response*, 2019).

Organizations should follow these steps if a breach occurs:

* A member of the staff should notify the response team if he or she detects, finds, or reports a breach.
* (Response team) members who responded to the data breach
* What steps should be taken by the response team (*Data Breach Response*, 2019).

A written data breach response plan will ensure that your employees are aware of the steps to be taken in the event of a data breach. Regularly reviewing and testing your strategy will ensure that it is up to date and that your employees are aware of their responsibilities. You need to take into account a variety of factors when determining what constitutes "regular" in this sense, including the size and nature of your company, the potential negative effects of a breach on a person, as well as the amount and sensitivity of the information you store when storing it (*Data Breach Response*, 2019).

**Need of Data Breach Response Policy**

Organizations are vulnerable to cybersecurity incidents because they have to respond quickly without disrupting the business. This makes responding to cyber threats difficult. The organization's reputation is at stake , leading to severe damage due to data breaches. IBM Security and Ponemon Institute reported that healthcare data breaches cost $9.23 million on average (How to Implement a Cyber Incident Response Plan for Healthcare, n.d.).

During the first few hours, a lot can go wrong. There is a possibility of destroying evidence. Communication can be sent that you wish you could take back, and containment does not always go as planned. Often, an incident will grow significantly after it is discovered, even though it could have been averted by taking some simple practical measures .Considering the data breach scenario in a Healthcare domain, the patient’s protected data are at stake which includes medical reports, personal information, insurance information, prescriptions, treatments, family medical details, clinic details, hospital and its each and every employee information, and so on . Also the HHS must be notified of healthcare data breaches impacting over 500 individuals, which could even result in fines. Data breaches are publicly disclosed on the Office for Civil Rights' (OCR) data breach portal once they are reported. Given the possible reputational damage, interruptions in patient care, and expensive expenditures that can arise from a healthcare data breach, developing and implementing a comprehensive incident response strategy is worthwhile, in every domain to avoid such extra expense, and also helps prevent future breaches (How to Implement a Cyber Incident Response Plan for Healthcare, n.d.).

Hence, every organization needs a plan for responding to data breaches. The success of your reaction is frequently dependent on the activities you take within the first 24 hours of learning about a data breach. A prompt response can significantly lessen the impact on the impacted parties (How to Implement a Cyber Incident Response Plan for Healthcare, n.d.).

**Response plan**

The more detailed the plan, the quicker it will be possible to react to a potential breach and lessen any hurt or damage done to those whose personal data has been exposed.

* Data breach detection, control, and management strategies.
* When a breach occurs, your staff, especially your response team, should take the following steps:
* Implementing those strategies is a priority, so ensure you have the capabilities to do so(“Effective Emergency Response Plan [+ Template] — Step-by-Step Guide,” n.d.).
* Communications that enable prompt alerts of relevant entities and concerned parties in a fast and transparent manner
  + Communication strategy: whose responsibility is it?
  + Establishing how affected people will be contacted and managed
  + Law enforcement agencies, cyber security organizations, regulators (such as the OAIC), and the media are among the outside parties that should be alerted
  + How does the decision to contact external stakeholders get made?
  + Who is responsible for maintaining communication with those external stakeholders?
  + The contact information for reporting any suspicions of a data breach, along with who needs to be notified right away.
  + When the breach should be escalated to the response team and under what conditions a line manager can handle it(“Effective Emergency Response Plan [+ Template] — Step-by-Step Guide,” n.d.).

This could take into account answering the following queries:

* Is the breach or suspected breach affecting several people?
* Does there exist a genuine risk that the affected person(s) will suffer substantial harm (now or in the future)?
* Do your practices or procedures have a systemic issue as a result of the breach or alleged breach?
* Other considerations that are pertinent to your situation, like the importance of the data to you or concerns about reputational risk.
* Who gets to decide whether or not the breach needs to be escalated to the response team?
* Documenting security breaches. It's important to think about how to document data breaches, particularly those that are not reported to the response team.
* A plan to determine and correct any data processing flaws that led to the breach.
* A technique for evaluating the effectiveness of your data breach response plan and your entity's response to the data breach after it has occurred (“Effective Emergency Response Plan [+ Template] — Step-by-Step Guide,” n.d.).

A reaction team is necessary to make sure that the pertinent personnel, roles, and duties are identified and recorded before the data breach occurs. If you wait until the breach has already happened before thinking about how to put together a response team, time may be lost. The company and the nature of the breach will determine the composition of your response team. For one breach against another, different skill sets and personnel may be required. You might need to add outside professionals to your team, such as for legal counsel, data forensics, and media management, depending on the size of your organization and the type of breach. Determine the kind of knowledge you might require and make sure it will be readily available when you need it.

Maintain an updated list of the team members, together with their roles, duties, and authority, as well as their contact information (perhaps related to the plan). In the event of organizational changes, you should make sure contact lists are updated. Each team member's position should have a backup contact person in case the primary one is unavailable. You might want to think about assembling a core team first and then adding additional members as needed.

Typical team roles and skills might include:

* Team Leader (Should oversee reporting to high management while managing the team)
* Project Manager (to coordinate the team and provide support to its members)
* Legal Support Risk management support ICT support/forensics support
* Information and records management expertise
* Media/communications expertise (to help in dealing with the media and external stakeholders, as well as helping in communication with those who are affected.

**Maintaining open communication between legal and IT teams**

The legal and IT teams have different perspectives on what is essential in the business. The skills they possess are unique to them. There is some advance coordination required to resolve the incident since it crosses both fiefdoms (How to Implement a Cyber Incident Response Plan for Healthcare, n.d.).Data breach incidents require the cooperation of both the legal and IT departments, which means they must develop an incident response plan that considers both the consequences and considerations of both.IT teams aren't usually thinking about the company's contractual obligations when they classify the risk of an incident when responding to an incident. There is a possibility that they do not fully understand the legal implications (How to Implement a Cyber Incident Response Plan for Healthcare, n.d.).

On the other hand, legal doesn't always understand the technical realities of security incidents. In other words, they might envision a process that isn't as technically sound or doesn't think about what needs to be done to protect the company's actual systems. Drafting an incident response plan gives those two groups the opportunity to figure out how they should interact and develop a strategy. A successful incident response plan requires collaboration between teams from all disciplines within an organization. An organization should adjust its incident response plan to reflect the change if it moves from on-premises data centers to cloud-based storage architecture, for example. It’s really helpful for them to review their incident response plan at least once a year to make sure it still applies(How to Implement a Cyber Incident Response Plan for Healthcare, n.d.).

**Identifying, Tracking and Containing the breach**

In the event of a security breach, organizations typically strive to contain and eradicate the issue as soon as possible. In some cases, this can result in hasty decisions, the destruction of evidence, or a loss of critical data. Having a predetermined incident response plan that guides organizations through a breach response from start to finish is therefore crucial (How to Implement a Cyber Incident Response Plan for Healthcare, n.d.).

Identifying, tracking, and responding to security incidents are critical components of an incident response plan. Despite the fact that this basic structure may be applicable to all organizations, each healthcare entity's tactics may differ depending on the critical data they possess, where the data is stored, and which key players will participate in the response team. Organizations should have policies in place for evaluating whether an incident is or is not a security incident, at what stage of the incident's lifecycle the incident is discovered, and whether it is malicious. Creating procedures for tracking and containing security threats should be the next step for organizations (How to Implement a Cyber Incident Response Plan for Healthcare, n.d.).

Developing an escalation path, or a procedure, to manage decision-making workflows so a problem can be solved as quickly and efficiently as possible. As the severity of the event increases, it may escalate to the CEO, the general counsel, or a working group. Assuring that the right people are involved at the right time is achieved by creating an escalation path (How to Implement a Cyber Incident Response Plan for Healthcare, n.d.).

**Notifying Affected Individuals**

In the event of a security incident, healthcare organizations are required to notify individuals who have had their PHI inappropriately accessed, acquired, used, or disclosed. It is mandatory to send breach notification letters, regardless of the number of people affected, within 60 days of discovering the breach. Healthcare organizations should send notifications as quickly as possible, despite the maximum time limit of 60 days (Preparing for the Inevitable: Security Incidents and Data Breaches | MedPro Group, n.d.).

There should be information in the breach notification letter about the nature of the breach, the data compromised, the measures the healthcare organization is taking to address the issue and reduce damage, how the organization intends to prevent future incidents, and how individuals can limit harm as a result of the breach. In the letters, recipients should find contact information that can be used to get in touch with the organization. Also according to the HIPAA Breach Notification Rule, breach notification letters must be sent via first-class mail, or alternatively, by email if the affected individual has consented to receiving them electronically (Preparing for the Inevitable: Security Incidents and Data Breaches | MedPro Group, n.d.).

The organization is also required to post notice of the breach on its website for at least 90 days if it has inadequate or outdated contact information for 10 or more affected individuals. It is also possible for the organization to provide notice of the breach to major print and broadcast media in the areas where the affected people live. As well, healthcare organizations should check whether state-specific breach notification laws apply, including requirements for expedited notification and credit monitoring services (Preparing for the Inevitable: Security Incidents and Data Breaches | MedPro Group, n.d.).

**Implementing A Communications Strategy**

Organizations can avoid miscommunication with stakeholders and customers by implementing an effective communications strategy. It’s common to create a legal record when responding to an incident, which can have significant consequences for the company. It is common for legal to be the last group consulted. Emails may have already been sent to customers or employees by the time they are brought in, and others may have already performed analysis that wasn't protected by attorney-client privilege (How to Implement a Cyber Incident Response Plan for Healthcare, n.d.).

In order to notify patients and employees of breaches, healthcare organizations should collaborate with their legal departments. The HHS Secretary and prominent media outlets must also be notified within 60 days of the breach if it has impacted more than 500 individuals. A notice about the breach should also be posted on the home page of the impacted entity's website.In this aspect of an incident response plan, organizations can benefit from working with a legal team (How to Implement a Cyber Incident Response Plan for Healthcare, n.d.).

**Documentation**

In the case of a security incident where confidential data is exposed, healthcare organizations must not only respond, but also document their actions for record-keeping and auditing purposes. It is important to provide details about:

* An analysis of the incident determines what happened and how it happened
* In response to the data breach, how the organization reacted
* Whether notifications were sent to affected individuals (including evidence that they were received)
* Data breaches affecting more than 500 people should be reported to HHS, state authorities (if applicable), and the media (if applicable) (Preparing for the Inevitable: Security Incidents and Data Breaches | MedPro Group, n.d.).

A healthcare organization should document details about a security incident, even if confidential information is not exposed, as well as evidence supporting their decision not to send breach notifications. As part of CIRCIA, healthcare organizations should also document their notifications to DHS of any cyberattacks (Preparing for the Inevitable: Security Incidents and Data Breaches | MedPro Group, n.d.).

**Planning corrective actions and training staff**

As a result of analyzing a security incident, vulnerabilities in systems and processes may be identified as well as opportunities to strengthen security protocols. In order to prevent similar events and other types of security lapses, healthcare organizations should address the factors that led to the incident. Regulatory bodies and government agencies expect to see that security vulnerabilities are addressed within a few days of a breach of protected health information, according to the HIPAA Journal. HIPAA fines don't necessarily apply when data is breached, but if security risks go unaddressed, they will (Preparing for the Inevitable: Security Incidents and Data Breaches | MedPro Group, n.d.).

It is also important to use the knowledge gained from the analysis of security incidents and data breaches to inform staff education and training. Employees with specific responsibilities in relation to the security protocols should be familiar with the organization's security plan and incident response procedures. In response to a security threat, tabletop exercises and drills can help reinforce a coordinated, quick response (Preparing for the Inevitable: Security Incidents and Data Breaches | MedPro Group, n.d.).

### 

### **Practicing The Plan**

An incident response plan should be practiced regularly as much as it is to have one in the first place. In order to prepare for security incidents, organizations can develop training programs and conduct incident simulations. The implementation of technical and administrative safeguards is a necessary step for HIPAA-covered entities. Although having a plan to respond to a data breach is one thing, implementing the plan effectively is another. An organization's incident response plan should be practiced regularly, cross-functional collaboration encouraged, and mitigation strategies developed for every possible security scenario. Further, a data breach can distract healthcare organizations from their primary duty, which is to provide patient care. Data breaches and security incidents are the worst kind of security breaches. That is why you need a robust security program. Data breaches usually cause big financial damage to companies, as well as reputational damage, as well as response and mitigation costs (How to Implement a Cyber Incident Response Plan for Healthcare, n.d.).

**Negative Impact**

Having an entity outside your company access your network and possibly proprietary information could be one of the biggest disadvantages. Adding this level of risk increases the risk. The vulnerability of infrastructure is increased when someone with external access has access to it. By exploiting the hole created in the third party's breach, cybercriminals could potentially gain access to your network (Cipher, 2018).

Also, customer trust is jeopardized and without credential hurt, there is no possible treatment, possibly upcoming security costs, Policy doesn't ensure security against the subsequent breach. Losing the confidence of customers is perhaps the most serious long-term impact of a major data breach even after having a strong data breach response policy. 92% of consumers think that businesses must take proactive steps to secure customer data, according to a PwC survey that looked at consumer opinion around cybersecurity and privacy risks. Since a firm must continually struggle to develop and preserve the integrity of its brand, a strong reputation is frequently its most valuable asset. Even the strongest reputations can be damaged by a single compromising incident, such as a data leak after having a policy.

**Positive contribution**

By developing a thorough data breach response strategy, businesses can get ready for a cybersecurity assault. A data breach response policy, often referred to as a data breach response plan, security breach response plan, or cyber incident response plan, assists organizations in effectively responding to a cybersecurity assault by outlining the required procedures to take in a clear, documented manner. There are different templates for data breach response policies that may be used; their lengths range from a few pages to several hundred pages, depending on the size of the firm. There are several items that any security breach response plan typically includes, even if the specifics may and should be tailored to the organization (Murphy, 2019).

#### 

#### **The Conclusion**

It is no longer enough to focus on trying to prevent unintentional access or exposure of proprietary systems or confidential information. Organizations should leverage a comprehensive solution to proactively manage a data breach. Being prepared puts you in a stronger position to protect your customers and ensure ongoing trust in your brand. The average time taken to identify a data breach is 196 days (over 6 months). Once organizations identify a breach, they must decide how to respond. This could take several months, so you should assess the impact on your day-to-day operations if you choose to run this process internally (*Benefits of a Data Breach Response Plan That Empowers Consumers | TransUnion Canada*, n.d.).

Whereas implementing this policy gives a handy to do list which is more efficient and saves time by reducing the inconvenience of finding a new route for remedy. Albeit data restoration and retention, this policy faces a challenge when it comes to safeguarding the reputation put on stake due to leak of media files that includes sensitive or personal pictures, screenshots, audio, and videos of confidential conversations etc. Which is already downloaded by the third party. Because in this case our policy cannot access neither can it find the device/s on which the content is downloaded. The credentials of finances too once lost and used cannot be recovered always.

Although this policy provides the user, customer and organizations with a significant comeback, there are some aspects of data breach response policy regarding media and finances that the cyber world need betterment to effectively claim the dominance of this policy in the world of cyber security. This can only be done by amalgamation of technology and innovative solutions.

**Reference**

1. *Benefits of a Data Breach Response Plan That Empowers Consumers | TransUnion Canada*. (n.d.). Retrieved December 2, 2022, from <https://www.transunion.ca/blog/data-breach-response-plan>
2. Cipher. (2018, November 5). The Pros and Cons to Outsourcing Incident Response. *Security Boulevard*. <https://securityboulevard.com/2018/11/the-pros-and-cons-to-outsourcing-incident-response/>
3. *Data Breach Response: A Guide for Business*. (2019a, April 29). Federal Trade Commission. <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business>
4. *Data Breach Response: A Guide for Business*. (2019b, April 29). Federal Trade Commission. <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business>
5. *Data Breach—Definition*. (n.d.). Retrieved December 2, 2022, from <https://www.trendmicro.com/vinfo/us/security/definition/data-breach>
6. Effective Emergency Response Plan [+ Template]—Step-by-Step Guide. (n.d.). *AlertMedia*. Retrieved December 2, 2022, from <https://www.alertmedia.com/blog/emergency-response-plan/>
7. *How to develop a data breach response plan: 5 steps | TechTarget*. (n.d.). Security. Retrieved December 2, 2022, from <https://www.techtarget.com/searchsecurity/feature/How-to-develop-a-data-breach-response-plan-5-steps>
8. *How to Implement a Cyber Incident Response Plan for Healthcare*. (n.d.). Retrieved December 2, 2022, from <https://healthitsecurity.com/features/how-to-implement-a-cyber-incident-response-plan-for-healthcare>
9. Murphy, D. (2019, November 26). *Best Practices for Your Data Breach Incident Response Plan*. Lepide Blog: A Guide to IT Security, Compliance and IT Operations. <https://www.lepide.com/blog/best-practices-for-your-data-breach-incident-response-plan/>
10. *Preparing for the Inevitable: Security Incidents and Data Breaches | MedPro Group*. (n.d.). Retrieved December 2, 2022, from <https://www.medpro.com/security-incidents-data-breaches>
11. Rd, L. U. C. · 1032 W. S., Chicago, & Policy, D. 2022 · P. (n.d.). *Data Breach Response Policy: Information Technology Services: Loyola University Chicago*. Retrieved December 2, 2022, from <https://www.luc.edu/its/aboutits/itspoliciesguidelines/DataBreachResponse.shtml>