HHS Breach Reports Analysis

Please read your assigned reports and answer the following questions.

Terms used:
HHS: The U.S. Department of Health and Human Services
HIPAA: Health Insurance Portability and Accountability Act of 1996
CE: Covered Entity
BA: Business Associate
PHI: Protected Health Information
ePHI: Electronic Protected Health Information
OCR: Offices of Civil Rights

* Required

Details of the Breach

1. **Pseudo ID:** *

2. **Breach ID:** *

3. **Who was responsible for the breach?** *
   Check all that apply.
   - [ ] The CE
   - [ ] Employee(s) of the CE
   - [ ] Business Associate (BA)
   - [ ] Employee(s) of the BA
   - [ ] Subcontractors
   - [ ] Other:

Types of Breach

Hacking/IT Incident:
- if electronic protected health information (ePHI) was impermissibly accessed through technical intrusions (including by malware or directed hacking) to the covered entity's or business associate's systems, servers, desktops, laptops, mobile devices, etc.

Improper Disposal:
- if the electronic media (servers, desktops, laptops, back-up tapes, thumb-drives, mobile devices, copiers, or other hardware) was not appropriately cleared, purged, or destroyed, or if paper records were not appropriately shredded or otherwise destroyed prior to disposal.

Loss:
- if equipment (servers, desktops, laptops, back-up tapes, thumb-drives, mobile devices, copiers, or other

hardware) or if paper records were lost, or if you believe they were lost. For example, select “Loss” if a workforce member left a laptop or paper records in a public place.

Theft:
- if equipment housing electronic protected health information (servers, desktops, laptops, back-up tapes, thumb-drives, mobile devices, copiers, or other hardware) or if paper records were stolen, or if you believe they were stolen. If electronic protected health information was stolen as a result of a technical intrusion, choose "Hacking/IT Incident".

Unauthorized Access/Disclosure:
- if no other category applies. For example, select “Unauthorized Access/Disclosure” for a misdirected mailing or other communication.

4. **What is the type of this breach?** *
Check all that apply.

- [ ] Hacking/IT Incident
- [ ] Improper Disposal
- [ ] Loss
- [ ] Theft
- [ ] Unauthorized Access/Disclosure

5. **List the words or phrases that determine your answer to the above question (e.g. "stolen", "inappropriately accessed", "hackers gained unauthorized access").** *

_____

_____

_____

_____

_____

6. **The incident described in the above breach description is caused by malicious intent.** *
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

7. **The incident described in the above breach description is due to accidental human error.** *
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	◯	◯	◯	◯	◯	Strongly agree

8. **List the words or phrases that determine your answer to the above question (e.g. "accidentally", "sold the information to third parties").** *

9. **If PHI or ePHI was involved, what did it include (check all items that apply)?** *
Check all that apply.

- [ ] Names, dates, or physical addresses
- [ ] Phone numbers
- [ ] Email addresses
- [ ] Social Security Numbers
- [ ] Financial information (e.g. credit card number)
- [ ] Clinical information (e.g. medical records)
- [ ] Other identification information (e.g., patient account number)
- [ ] Not mentioned
- [ ] Other:

Actions Following the Breach

Check the actions that the CE (or other parties) performed. Base your answers on the breach reports only.

Note that the choices are not mutually exclusive. One action may qualify for more than one choice.

10. **Recovery actions. The responsible parties would not and were not required to perform these actions if there was no breach.** *

Check all that apply.

- [ ] Notification: to affected individuals
- [ ] Notification: to HHS
- [ ] Notification: to law enforcement
- [ ] Notification: to the media
- [ ] Investigation: hire lawyers
- [ ] Investigation: (hire third parties for) security investigation
- [ ] Investigation: (hire third parties for) risk analysis
- [ ] Investigation: others
- [ ] Retrieval: hire agencies for retrieval
- [ ] Retrieval: unsuccessful retrieval attempt
- [ ] Retrieval: successful retrieval
- [ ] Sanction: employees
- [ ] Sanction: BA or subcontractor
- [ ] Sanction: others
- [ ] Compensation: call center for questions
- [ ] Compensation: credit monitoring
- [ ] Compensation: website for information
- [ ] Retraining or memorandum to corresponding staff (existing policies/procedures)
- [ ] Other: _____

11. **Preventive actions. The responsible parties were required to perform these actions regardless of, or before, the breach.** *

Check all that apply.

- [ ] Disposal: proper disposal of physical documents
- [ ] Disposal: proper disposal of electronic documents
- [ ] Physical safeguards improvement: workstations with ePHI
- [ ] Physical safeguards improvement: workstations with PHI documents
- [ ] Physical safeguards improvement: limited physical access to workstations
- [ ] Physical safeguards improvement: protection of mobile devices
- [ ] Physical safeguards improvement: encryption of physical documents
- [ ] Physical safeguards improvement: new policies
- [ ] Physical safeguards improvement: new procedures
- [ ] Technical safeguards improvement: limited access (e.g. password protection, authentication process)
- [ ] Technical safeguards improvement: encryption of ePHI or devices with ePHI
- [ ] Technical safeguards improvement: anti-virus software or procedures
- [ ] Technical safeguards improvement: new policies
- [ ] Technical safeguards improvement: new procedures
- [ ] Obtaining/requesting/assisting of BA's compliance
- [ ] Obtaining/requesting/assisting of subcontractor's compliance
- [ ] Other: _____

12. **Follow-up actions. The responsible parties performed these actions after the preventive actions.** *

Check all that apply.

- [ ] Hire/organize a team to ensure compliance
- [ ] Train employees (of the new polices and/or procedures)
- [ ] Upgrades of current systems
- [ ] Assurance to OCR of the corrective actions
- [ ] Comprehensive security audit for other improper uses or vulnerbalities
- [ ] Other: _____