Table 1: Classification of Reported Breaches into Categories

Source of Breach	Criteria for Inclusion	Example Entries
Carelessness/Negligence[a]	• Generally used terms such as "inadvertently" and "accidentally" • Exhibited the common trait of unintentional violation of established policies	• *"The covered entity (CE) … reported that its business associate (BA) … impermissibly mailed the protected health information (PHI) of 802 individuals to the wrong recipients."* • *"…a workforce member inadvertently emailed a spreadsheet containing the protected health information…"* • *"… emailed patients without using the blind-copy function…"*
Phishing and ransomware[a]	• Explicitly stated phishing or ransomware as the primary cause of the breach	• *"… reported that its business associate (BA) experienced a ransomware attack affecting the electronic protected health information (ePHI) of approximately 15,680 individuals."* • *"… an employee was the victim of an email phishing scheme that affected the electronic protected health information (ePHI) of 685 individuals."* • *"The covered entity's (CE) computer system was attacked by a ransomware virus that encrypted files … and damaged the network operating system rendering all of the CE's files unusable."*

Technical improper disclosure[a]	• A result of coding impropriety, software bugs, and insecure configurations that led to PHI exposure • Generally described as occurring due to technical errors or misconfigurations	• *"The covered entity (CE) … reported that unauthorized individuals accessed protected health information (PHI) due to a system administrator's incomplete installation of a web content management platform."* • *"…the business associate (BA), reported that an employee inadvertently misconfigured the settings on one of its computer servers, which made the server accessible over the Internet."* • *"The covered entity (CE) … reported that a programming error exposed the electronic protected health information (ePHI) of 11,536 individuals via its mobile application."*
Cyber-attack or external hacking attempts[b]	• Generally used terms such as "victim of a cyber-attack" and "hacking attempt" by external threat actors towards the organization • Unlike phishing or ransomware, there were no clear enabling actions by employees, vendors and other internal actors	• *"…the covered entity (CE), reported that it was the victim of a cyber-attack involving the electronic protected health information (ePHI) of 20,418 individuals…"* • *"The covered entity (CE), … reported that its business associate (BA) … was the victim of a cyber-attack involving the electronic protected health information (ePHI) of 33,730 individuals."* • *"the covered entity (CE) … discovered a cyber-attack as the malware was in the process of encrypting information in*

		the CE's computer system. … Its investigation revealed that the cyber-attack's likely entry point was via remote desktop connection."
Malicious insider[b]	• Described direct actions by an employee or business associate that facilitated a cyber breach for personal gains or the enrichment of another individual/entity	• *"…an employee emailed the protected health information (PHI) of 950 individuals to other members of a research study without authorization."* • *"…an employee … was arrested for fraud and the CE subsequently determined that she impermissibly accessed and used at least one patient's protected health information…"* • *"…an employee improperly disclosed protected health information (PHI) with the intent to sell it to an unauthorized third party."*
Theft	• Described incidents such as burglary and physical theft by external actors	• *"…the covered entity (CE), reported that a computer was stolen that contained 27,113 patients' files of a newly acquired medical practice…"* • *"…unknown persons broke into the covered entity's (CE) legal and audits offices, ransacked the offices and paper files, vandalized property, and started a fire that set off the building's*

	sprinkler system, which caused water damage to many documents and workstations." • *"…the covered entity (CE), reported that documents containing the protected health information (PHI) of approximately 616 individuals was stolen during looting due to civil unrest…"*

[a]Unintentional human factors.
[b]Malicious human factors.