Data Security Breach Incident Response Checklist

Step #	Tasks	Resources (Name or Department) and Task Start Date and Time	Complete (Yes/No)	Completion Date
1	**Identify Individuals/Entities of Data Theft / Build Notification List**			
1.1	Conduct Forensic Analysis to Identify Individuals/Entities Names, Addresses, Email Addresses and Types of Data Stolen **NOTE**: We must notify **ALL** individuals identified by the Forensic Analysis effort. Therefore, ensure there is an accurate count of **ALL** identified Individuals/Entities and that their contact information (i.e., email addresses and postal mail addresses) are on file and up-to-date because this information will be used for the notification processes in sections 3.3 and 3.4 below.			
1.2	Cross-Reference List of Data – Compile most-recent contact addresses			
	1.2.1 Cross Reference with HRMS			
	1.2.2 Cross Reference with Student Information System			
	1.2.3 Cross Reference with Procurement System			
	1.2.4 Cross Reference Other University Systems (Please List)			
	1.2.5 Cross Reference with External Address Location Services			
1.3	**Add QA Test Contact Data for External Call Center**			
1.4	Establish a budget # / index number for tracking costs to a central account, e.g., call center, postage, stationary, toll free calls, long- distance calls, equipment / furnishings for call center, overtime.			
1.5	File a police report, maintain the police report #, report date, and incorporate this data into the Call Center scripting in case individuals/entities ask for these details. (If applicable)			
1.6	Remediation (refer to a separate list/chronological log of actions taken)			
2	**Call Center:** *External vs. Internal -- Business decisions: consider breach size (# of individuals/entities & type of data), anticipated call volume, sensitivity of data, hours / days of call coverage and internal resources, costs.*			
2.1	**External Call Center**			
	2.1.1 Prepare contract with External Call Center Vendor + HIPAA BAA (if required)			
	2.1.2 Sign contract with External Call Center + & Require signed Confidentiality / Nondisclosure Agreement			
	2.1.3 Establish 800 number + from / to hours			

Data Security Breach Incident Response Checklist

Step #	Tasks	Resources (Name or Department) and Task Start Date and Time	Complete (Yes/No)	Completion Date
	2.1.4 External Call Center Ramp-up			
	2.1.4.1 Provide Call Center with scripts including plans for escalation of Calls			
	2.1.4.2 Establish clear QA processes			
	Create QA data to be included in data feeds so we can assess call quality without impacting true impacted individuals			
	2.1.4.3 Send data about individuals/entities of the data theft to the Call Center, so Call Center staff can identify them (and for programming their systems). Includes QA data			
	2.1.4.4 Define documentation and reporting requirements for and from Call Center			
	2.1.4.5 Define process for callback/escalation. Establish incoming institution's email address for the escalations. Integrate escalations with institution's systems used in 2.x (Internal Call Center).			
	2.1.4.6 Conduct training of Call Center staff			
	2.1.4.7 Identify designated internal staff who will participate in the Quality Assurance testing of the External Call Center. Establish QA procedures and criteria.			
	2.1.5 Institution conducts initial testing to ensure correct messages and escalation are being employed.			
	2.1.6 Launch external Call Center (date / time)			
	2.1.7 Monitor and conduct on-going QA of external Call Center			
	2.1.8 Ongoing Review External Call Center QA			
	2.1.9 Continue to analyze QA results			
	2.1.10 Analyze response statistics from Call Center			
2.2	**Add QA Test Contact Data for External Call Center**			
	2.2.1 Identify internal staff to work in the Call Center + set Call Center Hours Hours: During week #1 prepare mgr coverage for add' hours (7:00AM-8:00PM PST). Triage long-winded calls to a manager so as not to tie up incoming lines.			
	2.2.2 Establish campus location for the Call Center, location should be in close proximity to managers for help with call escalation questions.			

Data Security Breach Incident Response Checklist

Step #	Tasks	Resources (Name or Department) and Task Start Date and Time	Complete (Yes/No)	Completion Date
	2.2.3 Install: Computers, telephones (multi-line with line appearance display), phone headsets, furniture, whiteboard, fax machine, printer, chairs and other equipment and establish incoming toll-free numbers and long-distance code for return calls.			
	2.2.4 Identify tracking and reporting system to use for Call Center			
	2.2.5 Set up tracking system for Call Center, including ID's for all agents and response managers			
	2.2.5 Identify staff who will participate in the Quality Assurance testing of the Internal Call Center			
	2.2.6 Provide Call Center staff with Scripts			
	2.2.7 Train Call Center staff			
	2.2.8 Conduct QA Testing of Staff by conducting simulated calls			
	2.2.9 Monitor and conduct on-going QA of Internal Call Center			
	2.2.10 Create institution's email address & determine who will respond to emails from individuals/entities (email scripts)			
	2.2.11 Timing for 1st calls: Expect calls to start arriving 24 hours after mailing, be prepared.			
	2.2.12 Establish an internal call center database or list to manage incoming calls and where call backs are needed.			
	2.1.13 Notify Credit Bureaus in advance -- as a "courtesy heads-up notice to expect calls".			
3	**Communications**			
3.1	**Add QA Test Contact Data for External Call Center**			
	3.1.1 Identify Communications that need to be created			
	3.1.2 Identify who from institution will be participating in the response			
	3.1.3 Coordinate response planning with partner institutions effected by incident.			
3.2	**Add QA Test Contact Data for External Call Center**			
	3.2.1 Internal and External FAQ's			
	3.2.2 Press release - Draft and launch via designated spokesperson			

Data Security Breach Incident Response Checklist

Step #	Tasks	Resources (Name or Department) and Task Start Date and Time	Complete (Yes/No)	Completion Date
	3.2.3 Drafts of notification letters to various segments of the impacted individuals/entities audience			
	3.2.4 Call center scripts			
	3.2.4.1 External Call Center			
	3.2.4.2 Internal Call Center			
	3.2.5 Communications to employees, vendors and businesses partners			
	3.2.6 Timeline for web site			
	3.2.7 “Resource" and "Reference" page for web site			
	3.2.8 Introductory piece for web site			
	3.2.9 Escalation guide for call center			
	3.2.10 Internal communications to leadership & advisory groups			
	3.2.11 Notification to institution's switchboards/operators, security, frontline staff			
	3.2.12 Formal Notification to Office of Alumni and Development			
	3.2.13 Notification to vendors/suppliers (e.g. insurance, etc.).			
	3.2.14 Communication for internal stakeholders likely to have contact with individuals/entities			
3.3	**Send Out Notification E-mails** *(will happen in waves based on getting the best data available from various data stewards)*			
	3.3.1 Identify e-mail addresses			
	3.3.2 Identify mechanism for sending e-mails			
	3.3.3 Identify which recipient receive which e-mails			
	3.3.4 Prepare email recipient list(s)			
	3.3.5 Send out e-mails to data theft individuals/entities			
3.4	**Send out Traditional U.S. Mail Letters** *(will happen in waves based on getting the best data available from various data stewards)*			
	3.4.1 Identify vendor / mail house to send out letters			
	3.4.2 Decide on which institution letterhead to use, which return address, signature			
	3.4.3 Order institution stationary + window envelopes			
	3.4.4 Prepare mailing list of Individuals/Entities who should receive letters and which letters they should receive. Decide whether to include a page of FAQs.			

Data Security Breach Incident Response Checklist

Step #	Tasks	Resources (Name or Department) and Task Start Date and Time	Complete (Yes/No)	Completion Date
	3.4.5 Send final wording for the letter(s) to the Mail House Vendor for mail-merge			
	3.4.6 Send the Mailing List to the Mail-House Vendor with individual/entity addresses and indicate type of letter to be sent to each recipient. Excel file: one data element per column: Mr/Ms, first name, last name, street addr1, street addr2, city, state, zip			
	3.4.7 Vendor prepares letters for mailing. For large mailings, Vendor will vet the address list to the "National Change of Address" (NCOA) clearinghouse (US Postal Service) to expedite delivery. Determine if you need to be informed of address changes. Process is sometimes referred to as "cleansing the mail list".			
	3.4.8 Decide if the letters will be sent via bulk mail or 1st class postage			
	3.4.9 Send Out Letters			
	3.4.10 Instruct Mail House Vendor what to do with the mailing list afterwards			
	3.4.11 Assign a call center staff member to document "mail bounce- back letters" in the call center database, for tracking purposes.			
3.5	**Media Relations**			
	3.5.1 Campus Communications or Media Point person			
	3.5.1.1 Identify the Campus Point Person to talk to the media			
	3.5.1.2 Conduct media training for campus point person to talk to the media			
3.6	**Press Release**			
	3.6.1 Identify Recipients of the press release			
	3.6.2 Send out press release			
	3.6.2 Conduct press briefing			
3.7	**Campus Response Web Site**			
	3.7.1 Identify where to host Web Site			
	3.7.2 Identify name for the Web Site			
	3.7.3 Register the domain name for the web site			
	3.7.4 Build the web site			
	3.7.5 Test the web site			
	3.7.6 Launch the web site			
	3.7.7 Include the web-link in the notice to individuals/entities			
3.8	**Campus Communication**			

Data Security Breach Incident Response Checklist

Step #	Tasks	Resources (Name or Department) and Task Start Date and Time	Complete (Yes/No)	Completion Date
	3.8.1 Send out Leadership memo, e.g., senior business officers, deans, president's office			
4	**Policy and Legal Issues**			
4.1	Identify types of responses required by State / Federal laws and campus policy			
4.2	Consult with counsel to determine whether to provide a voluntary notice to State / Federal agencies			
4.3	Identify key policy questions to answer for response			
4.4	Determine answers for identified policy and legal issues			
	4.4.1 Will the campus offer identity theft insurance to the individuals/entities of the data theft?			
	4.4.2 What is the law regarding compensation for individuals who were victims of the data theft? What is the potential liability of the campus?			
	4.4.3 Did the institution violate any campus policies that led to the data theft?			
5	**Launch Response**			
5.1	Prepare readiness Check-list to launch response			
5.2	Fill out readiness Checklist			
5.3	Receive "O.K. for Launch" from project leads and University leadership			
5.4	Launch (date: MM/DD/YYYY)			
6	**Conduct Review of Response and Document Lessons Learned**			
6.1	Preventive approach in case of next incident			
6.2	Update checklist accordingly			