**SAMPLE HIPAA Breach Notification Action Plan DRAFT**

**11/1/17 60 Day Timeline begins**

**12/22/17 Covered Entity deadline**

**12/30/17 Report to Office of Civil Rights**

| **Task** | **Follow up** | **Due Date** | **Status** |
| --- | --- | --- | --- |
| Before a breach occurs, have in place:  Policies  Procedure  Reporting Structure | Are policy & procedure current? |  |  |
| HIPAA incident reported | To who?  Date you knew or should have known starts the clock | 11/1/17  C:\Program Files (x86)\Microsoft Office\MEDIA\CAGCAT10\j0234131.wmf |  |
| Begin HIPAA Incident Investigation | Form  Policy  Procedure |  |  |
| Determine if a Forensic Analysis is required | Do you have the capacity to do this in house? Do you have a Business Agreement with a vendor in place? | 12/5/17 |  |
| Send Forensic Report & recommendation to Legal, if required by CE | In house? Contracted? | 12/6/17 |  |
| Obtain written legal opinion, if required by CE | Breach or possible breach?  If no, document & file | 2/2018 |  |
| HIPAA Incident Report  Assess for probability of harm | If yes, assess  1  2  3  4 | 12/15/17 |  |
| Determine all necessary information | Who, What, When, Where, Why |  |  |
| Analyze required factors | Physical, Technical & Administrative Safeguards in place at time of the incident |  |  |
| Employee(s) involved  Policies  Training  Mitigation  Sanctions | Have a system in place that allows you to verify the employee has received all required steps | 12/15/17 |  |
| Maintain a draft a notification letter containing required elements |  | 12/15/17 |  |
| Customize the notification letter to the affected individual(s) |  | 12/13/17 |  |
| Maintain a toll free phone line |  | 12/18/17 |  |
| Address and mail notifications to clients by first class mail | Verify post mark dates on letters | 12/20/17 |  |
| Where will the costs be allocated |  |  |  |
| Draft a press release/substitute notice for public release |  | 12/20/17 |  |
| Publish press release/substitute notice on website | Be able to verify | 12/22/17 |  |
| Add to patient spreadsheet documentation of who calls, date, question and answer, who spoke with |  | 12/26/17 |  |
| Appoint staff to field inquiries |  | 12/20/17 |  |
| Notify OCR per HIPAA requirements | CE Privacy & Security Officer will enter OCR Breach Portal Information | 12/27/17 |  |
| Staff training and remediation | 2 all staff emails sent  11/21/17 Compliance Officer  12/19/17 SANS Ouch Newsletter sent to CE workforce  1/9/18 Pricing HealthStream training | 1/31/17 |  |
| 100 impacted patients currently inpatient @ CE. | HIPAA Liaison to train SWs to give the patient notification letter | 12/20/17 |  |
| LEGAL Office directed to make a CBI report | 12/21/17  Also reported to internal Security | 12/21/17 |  |
| Confirm mail sent with 12/22/17 postmark | Employee (303 866 3887) @ IDS (processes State mail) confirmed patient notification letters received in Denver from Pueblo & were stamped with 12/22/17 date | 12/22/17 |  |
| Review of entire OCR response |  | 12/22/17  C:\Program Files (x86)\Microsoft Office\MEDIA\CAGCAT10\j0234131.wmf |  |
| Organize materials with index and sections |  |  |  |
| Deliver 3 copies by deadline |  | 12/30/17  C:\Program Files (x86)\Microsoft Office\MEDIA\CAGCAT10\j0234131.wmf |  |
| 1st Response from OCR |  |  |  |
| 2/12/18 1st Response letter from OCR received | Complete Attachment A - DATA REQUEST 12 Items | 3/10/18 |  |
| 1. CE position regarding the allegations. |  |  |  |
| 1. CE most recent risk analysis performed for or by CE to identify potential risks and vulnerabilities (with appropriate risk level) to logical, physical and network security of the systems that store or contain electronic protected health information (ePHI). See 45 C.F.R. § 164.308(a) (1)(ii)(A). |  |  |  |
| 1. CE risk management plan, policies, and procedures used to implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level, based on the risk analysis. Include evidence of completed risk remediation actions. See 45 C.F.R. §164.308(a)(l)(ii)(B). |  |  |  |
| 1. CE sanctions policy and evidence of the sanction of the employee involved in the breach. See 45. C.F.R. § 164.308(a)(l )(ii)(C). |  | 2/15/18 COB Employee documentation |  |
| 1. CE policies and procedures related to its security awareness and training program. include a copy of the training's content and evidence that the responsible CE employee had participated in the security awareness and training program prior to the event. See 45 C.F.R. § 164.308(a)(S)(i ). |  |  |  |
| 1. CEs policies and procedure for guarding against, detecting, and reporting malicious software and CE response to the malicious software that gained access to the employee's computer and caused the subject breach. See 45 C.F.R. §164.308(a)(5)(ii)(B). | CE 15.01 Internet Usage |  |  |
| 1. A representative sample of the breach notification sent to the individuals whose unsecured ePHI has been, or CE reasonably believes to have been, accessed, acquired, used, or disclosed as a result of the loss of its laptop computer containing ePHI. See 45 C.F.R. §164.404. | Copy of Patient Notification Letter |  |  |
| 1. evidence that substitute notification occurred if more than ten of the breach notification letters to affected individuals were returned as undeliverable by the post office. See 45 C.F.R. § 164.404(d(2) . | Substitute notice provided via statewide media outlets |  |  |
| 1. CEs breach notification procedures addressing breach notification to individuals, media, and the Secretary. See 45 C.F.R. §§ 164.404(a), (b), (c), and (d);164.406(a),(b),and (c); and 164.408(a) and (b). |  |  |  |
| 1. At time of breach:   CEs relevant Privacy Rule policies and procedures addressing confidentiality of ePHI, safeguards, and mitigation. See 45 C.F.R. §§ 164...502(a); 164.308(b)(l) and (2); 164.504(e); and 164.530(c) and (f). |  |  |  |
| 1. Evidence of mitigation taken by CE to address the breach. See 45 C.F.R.§ 164.530(f). | Employee education, emails to all staff, evaluating training gaps |  |  |
| 1. any other information CE believes OCR may find useful in its investigation. |  |  |  |
| 2nd Response from OCR |  | July 27,2018 |  |
| 1. CE’ risk management plan, policies, and procedures used to implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level, based on the risk analysis. Include evidence of completed risk remediation actions. See 45 C.F.R. § 164.308(a)(1)(ii)(B). The risk management plan would address any risks identified in the risk analysis and provide a plan for addressing the risks, including the action to be taken, responsible party, and due date. |  |  |  |
| 1. CE policies and procedures related to its security awareness and training program. Include a roster of all the Pueblo State Hospital’s employees’ attendance for the required training. See 45 C.F.R. § 164.308(a)(5)(i). Although CE has provided copies of the training and attendance for the affected employee, we need to have a copy of the procedure that addresses training requirements and show attendance records for all staff. In your response, there were several items provided that indicated training was implemented, but there was no formal procedure. If you do not have a formal procedure, please provide your written assurance that a procedure will be developed and the date by which it will be completed. |  |  |  |
| OCR provided technical assistance via phone call |  | None |  |
| OCR Closing Letter | None | Received 8/31/18 | https://media5.picsearch.com/is?P3bAWtBLDRit4YoDQqTZMA1pzbV0Q6HwyyOuatMKecE&height=212 |