[redacted]

March 3, 2024

U.S. Department of Health and Human Services
Via Email: FOIArequest@hhs.gov

Freedom of Information Request Regarding “500” Markers in Breach Reporting

Dear FOIA Officer:

This is a Freedom of Information Act (FOIA) request regarding procedures and actions taken by the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) in response to HIPAA breach reports where entities initially report "500" or "501" patients affected. Because HHS’s online FOIA system is experiencing a problem with my account, I was asked to submit this directly via email.

Context and Background:

Under HIPAA regulations, covered entities are mandated to report breaches involving the protected health information (PHI) of 500 or more patients to HHS within 60 days of initial discovery. However, it appears some entities submit placeholder figures of "500" or "501" when the exact number of affected individuals is yet to be determined or can not be determined (as might be the case when ransomware encrypts email files containing PHI where there is no backup available or where threat actors maliciously delete all data).

Despite the requirement for entities to update or amend their reports with accurate figures once determined, it appears that many fail to do so, leading to potential underestimation of breach impacts and potential lapses in follow-up actions by HHS to ensure affected patients are duly notified.

A quick persual of HHS’s public breach tool found sixty-four (64) reports that appear to have used a 500 or 501 “marker” for number of patients affected for incidents that are still “Under Investigation” and an additional 138 reports from the “Archived” section with reports of 500 or 501. For 2023 alone, DataBreaches.net found 53 incidents with 500 or 501 markers that were never updated by the end of the year. Using the mean number of breached records per incident from other data, those 53 incidents might involve almost 10 million more patients than what HHS’s public breach tool might indicate.

In January 2024, this requestor sent emails and called HHS Media to ask them to explain what HHS does to follow up on “marker” report situations. Despite multiple emails and two phone calls with voice mails left over a period of weeks, no reply or even acknowledgement was received.

Records Requested

1. Any documents, policy statements, records, discussions, or correspondence pertaining to HHS OCR's procedures or protocols for following up on breach reports initially filed with "500" or "501" patients affected, where the actual number is likely to exceed the reported figure.

2. Any documents, policy statements, records, or materials outlining whether HHS ever suspects reported figures to be inaccurately low, and if so, the measures or actions it undertakes or plans to undertake to address such discrepancies.

3. Any documents, policy statements, records, or materials documenting instances where HHS OCR initiated enforcement actions or resolution agreements due to the failure of entities to update reported figures as required.

Thank you for your time. If this request requires clarification, please call me at 516-776-7756 and hopefully, we can clarify it quickly. I look forward to your prompt reply. My other contact information can be found at the top of this letter.