MID-ATLANTIC PERMANENTE Medical Group

Research Privacy Investigation Breach Risk Assessment

CONFIDENTIAL DOCUMENT

Name of the person completing form and date:		
Date Complaint Received:	**How Incident was reported:**	
date the incident first occurred (breach start date):	**Discovery Start (Date when KPMAS first learned about the incident):**	**LOCATION:**
Name of Principal Investigator:		**Name of Research Study:**
# of Affected members:		**Provide list of Medical Record Number(s):**
Name of the Person /Role who Disclosed PHI:		**Department:**
Name of the Person/Role who Received PHI:		**Department:**

BRIEF DESCRIPTION OF INCIDENT (INCLUDING TYPE (ORAL, WRITTEN, PAPER, ELECT) AND LOCATION OF BREACH INFORMATION

1. DESCRIBE THE NATURE & EXTENT OF THE PHI INVOLVED - TYPE OF IDENTIFIERS

Type of PHI and Identifiers	**Yes/No/NA**	**If Yes, Describe and likelihood of Re-identification:**
Non-Sensitive PHI / PII - Personal identifiers without SSN (address, phone number, email address, ISP, internet domain name) or a research limited data set[1]		

[1] A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses: (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; (xvi) Full face photographic images and any

Research Privacy Investigation Breach Risk Assessment

CONFIDENTIAL DOCUMENT

Enrollment Information - Eligibility status, enrollment/disenrollment date		
Billing Information - MRN, account number, DOS, EOB, procedure codes, diagnosis		
Patient Medical Information - Provider specialty, treatment, medication, diagnosis, test results, lab results, AVS, chart notes, referrals		
Sensitive Health Information - Genetics, communicable diseases, sexual disorders, weight loss or cosmetic surgery, cancer, Parkinson's or MS diagnosis, general anxiety or depression, etc.		
Specially Protected Information - HIV/AIDS, STD, chemical dependency, mental health treatment at BHS, such as major depression or bipolar disorder, reproductive treatment for minors, ADD or ADHD diagnosis or treatment, etc.		
Financial Information - Credit card or bank account number, security code, transaction dates, SSN, driver's license, associated with an individual's name		
2. DESCRIBE THE PERSON WHO USED THE PHI OR TO WHOM THE DISCLOSURE WAS MADE AND WHETHER THE PERSON WAS AUTHORIZED OR UNAUTHORIZED.		
Type of Person	**Yes/No/NA**	**If Yes, Describe and determine whether the person was authorized or unauthorized**
Member of Covered Entity - KPMAS workforce member, business associate, another health care provider, plan, or clearing house		
Non-Inflammatory Party - Family member, friend, another patient or member, non-covered entity, third party not associated with KPMAS or the individual		
Undesired Party - Media, unknown or lost, patient's or member's employer		
Inflammatory party - Ex-spouse, adoptive or birth parents, person involved in a crime or theft		
3. DESCRIBE THE EXTENT THE PHI WAS ACQUIRED, ACCESSED, VIEWED OR DISCLOSED		
Type of Scenario	**Yes/No/NA**	**If Yes, Describe:**
Viewed, heard (verbal), or opportunity only		
Acquired/viewed - Has/had physical custody of PHI, PHI given to the wrong patient, location unknown		
Intentional - Inappropriately accessed or obtained, transferred/disclosed. PHI exposed via a public web page		
4. DESCRIBE THE EXTENT TO WHICH THE RISK TO PHI HAS BEEN MITIGATED		
Type of mitigation	**Yes/No/NA**	**Is Yes, Describe:**
Mitigated with Forensic Evidence - Forensic analysis shows password protected, information encrypted and/or uncompromised data (except when encrypted by the unauthorized individual who acquired the PHI/PII)		
Mitigated with Documented Evidence - Assurance that PHI will not be further used or disclosed, data wiped from the device, information returned complete, information properly destroyed and attested to, electronically deleted.	**Yes**	
Mitigated with Limited Evidence - Information properly destroyed unattested or verbal attestation, electronically deleted but unsure of backup status, very low risk data on one or limited number of pts.		

comparable images. 45 C.F.R. § 164.514(e)(2).

Research Privacy Investigation Breach Risk Assessment

CONFIDENTIAL DOCUMENT

Unable to Mitigate - Sent to the media, unable to retrieve, on the internet for any period of time, unsure of disposition location, high suspicion or knowledge of PHI re-disclosure, transferred or otherwise compromised		
CONCLUSIONS: (SUBSTANTIATED, UNSUBSTANTIATED, INCONCLUSIVE)		
	Yes/No/ Inconclusive	**If yes or inconclusive, please describe:**
Were the Claims Substantiated?		
Was there conflicting or inconsistent information produced in the investigation?		
Were any company policies violated? If yes, reference the policies		
How was the credibility of the witnesses assessed? Please describe		
Do you believe/not believe the individual who raised the issue? Please describe		

STOP HERE: MAPMG COMPLIANCE DEPARTMENT WILL COMPLETE BREACH RISK ASSESSMENT

MAPMG Director of Compliance Recommendation to KPMAS IRB/Privacy Board

6. BREACH NOTIFICATION REQUIRED

EXCEPTIONS THAT DO NOT CONSTITUE A BREACH

PHI / PII was not involved in the event, the information was de-identified or no use or disclosure in violation of the Privacy Rule occurred?	**No**	**If Yes Stop**
Was it a good faith, unintentional acquisition, access or use of PHI by employee/workforce within scope of employment and not further acquired, accessed, used, or disclosed by any person?	**No**	**If Yes Stop**
Was it an inadvertent disclosure of PHI from one person authorized to access PHI to another authorized person within the entity or OHCA and not further acquired, accessed, used, or disclosed by any person?	**No**	**If Yes Stop**
Would the unauthorized person to whom PHI is disclosed (recipient) not reasonably have been able to retain the information?	**No**	**If Yes Stop**

BURDEN OF PROOF - An acquisition, access, use or disclosure in a manner not permitted is presumed to be a breach unless KPMAS or business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment.

Low probability Yes or No?	**If no, date letter (notice) provided?**
Disclosure accounting required? Yes or No	**Date sent to HIMS?**

MID-ATLANTIC PERMANENTE Medical Group

Research Privacy Investigation Breach Risk Assessment

CONFIDENTIAL DOCUMENT

MAPMG Director of Compliance Signature	Date: