



GARRETT LAW LLP

415.513.5035 • 120 Ward Street #1058 • Larkspur, CA • 94977

TO: Michael Anderson, Risk Manager
County of El Dorado

FROM: Linda Garrett, Esq.
Garrett Law LLP

DATE: June 13, 2022

RE: Summary of Work:
HIPAA Policy and Procedure Project
(May-June 2022)

The El Dorado County HIPAA Policy and Procedure Project (May-June 2022) required a review of existing policies and forms, and the revision, updating or creation of new policies and forms necessary to comply with federal and state laws (HIPAA, Part 2, CMIA, LPS Act, PAHRA, etc.). Many of the existing policies and forms needed updating to reflect recent changes in the law, for example the August 2020 and January 2021 changes to 42 CFR Part 2 federal substance use disorder regulations, the Ciox v. Azar case (2020), and the Office of Civil Rights “right of access” initiative launched in the Fall of 2019.

The documents that were included in the project are discussed below.

1. Policies and Procedures (82 pages, total)

- **Preamble to Policy and Procedures** - Edited, and updated; removed references to insurance plan obligations that do not apply to the County and could cause confusion to staff by inadvertently requiring them to do more work. (5 pages)
- **Part 1 - Administration** - Rewritten, and updated to reflect roles and responsibilities of HIPAA Privacy Official, HIPAA Security Official and HIPAA Compliance Committee; removed references to insurance plans and obligations of plans under HIPAA; clarified each requirement under the law and streamlined information in the policy. (8 pages)

- **Part 2 - Uses and Disclosures** - Heavily edited, rewritten, and significantly expanded and updated to describe the HIPAA minimum necessary rule, de-identification standards, and all HIPAA uses and disclosures, including the six main categories of uses and disclosures: two that are required, including 1) to the Secretary and 2) to the patient seeking access to their own record; and the four that are permissive: including 1) treatment, payment and operations, 2) written authorization, 3) verbal authorization, and 4) no authorization -- this was the area with the most additional new information, and each of the twelve types of disclosures that do not require patient authorization that are found at 45 CFR 164.512(a) through (l) was addressed.

The new policy language discussing each of the six main categories of uses and disclosures now includes specific limitations or conditions that would apply due to more stringent state law restrictions found in the LPS Act (providing more protections to mental health information), Health and Safety Code sections (providing greater protection for HIV test results), and federal protections under 42 CFR Part 2 (regulations that greatly limit disclosures of substance use disorder treatment program information).

Each of the more stringent exceptions is now described in detail in the policy, and direction is provided on how to proceed. In the case of complex disclosures such as research uses without consent of the patient, disclosures in response to criminal search warrants served by law enforcement, requests from US Homeland Security, or Court orders for SUD information, guidance was provided on notifying the HIPAA Privacy Official or seeking direction from the Office of County Counsel before proceeding, since these disclosures are subject to many limitations, criteria and thresholds, and each case should be individually considered. (21 pages)

- **Part 3 - Security Rule (New)** - Written to reflect both the HIPAA Security Rule at 45 CFR Part 164, Subpart C, and California Medi-Cal All County Letter 19-16, Privacy and Security Agreement (PSA), that was incorporated into the policy to specifically address protections for Medi-Cal personally identifiable information (PII); sections are now divided into the three specific types of safeguards (administrative, physical and technical), with each of the “required” and “addressable” safeguards within those three categories specifically listed and discussed. Additionally, language was added to address business associates and the responsibilities of HIPAA Security Officer to perform risk assessments, ongoing audits, and maintain documentation of those audits, staff training, and other compliance efforts. (21 pages)
- **Part 4 - Patients’ Rights** - Rewritten to reflect Ciox v. Azar and the DHHS Office of Civil Rights “right of access” initiative, including both HIPAA patients’ rights plus PAHRA rights, and adding the patient’s right to submit a 250 word addendum to their record under California state law. New forms were created to reflect the rights of patients regarding their PHI, and clarification of limits on the right to access PHI, amend the record, and request special privacy protections. (15 pages)

- **Part 5 - Breaches** - Part 5 was rewritten to reflect sanctions, mitigation, reporting and notification requirements triggered by 1) HIPAA, 2) State Law re: facilities and programs that are licensed by the state, and 3) Medi-Cal requirements; the policy now clearly outlines steps for reporting privacy breaches and security incidents, and clarifies guidance on how soon, and how, notification to the patient and reporting to government agencies must be done. A sample breach notification letter to the patient providing a template for that communication was created to support staff in their efforts to follow the breach notification requirements. (12 pages)

2. Forms/Templates (Appendices) (51 pages, total)

- **Appendix 1 -- Complaint Form** (Re-done) - This form was redone in 14 point font to be used by patients, staff or others; simplified; clarified how/where to submit.
- **Appendix 2 -- Patient Request for Access to Record** (New) - The new initiatives of OCR and the Ciox case make it important that the County make it easier, not more difficult, for patients to request access to their record (to inspect or get a copy); this form was created with that in mind.
- **Appendix 3 -- Authorization to Use, Disclose, Exchange PHI** (New) - The old form did not conform with Part 2 regulations, and was redone to be suitable for use by all disciplines and easily adaptable for multi-disciplinary team or multi-party exchange situations.
- **Appendix 4 -- Request to Amend/Correct Record** (New) - This new form clarifies the patient's right to correct errors in the record and simplifies the process while documenting the County's compliance with HIPAA.
- **Appendix 5 -- Request for Accounting of Disclosures** (New) - This new form reflects the patient's right to request a list of those entities and individuals who have had access to their record while clarifying the extensive exceptions available to the County (e.g., that disclosures for treatment, payment and operations, or at the request of the patient, do not have to be included on the accounting).
- **Appendix 6 -- Request for Special Privacy Measures** (New) - Though the policy cautions County staff against granting special privacy measures due to the difficulties that this could cause in assuring compliance and assuring that all staff are aware of the special limitations that have been agreed to, this form simplifies the process while providing clear documentation for the County should there ever be a dispute, for example, if a well-known member of the community requests "John/Jane Doe" status while receiving services from the County.

- **Appendix 7 -- Request for Alternative Communication (New)** - This form clarifies and documents the right of patients to make reasonable requests, and for the County to agree to reasonable requests, to communicate information such as appointment reminders to the patient in a particular format (e.g., by email only) or to a specific address, including which address(es) not to use (e.g., the patient's work address) for communication of health care or billing information.
- **Appendix 8 -- Sample Template: Breach Notification Letter to Patient (New)** - This tool was created to help staff prepare notification letters that must be mailed to patients using first class mail if there is a breach of the patient's protected health information; the tool includes every item that the law requires the County to address if a breach is discovered, and provides guidance on how to word the letter so that regret is appropriately expressed, without potentially problematic statements as to fault.
- **Appendix 9 -- Notice of Privacy Practices (New)** - Two Notices of Privacy Practices were reviewed, including the public health NPP document, and the information that is posted on the County website. Certain verbatim language required to be part of the notice was misquoted, and required elements were missing; editing was so extensive that a new NPP was written that could be used by County public health, and behavioral health programs. Note that the current behavioral health NPP has not been received and reviewed, and may be usable in its current iteration; or, it may need revision. It may be easier to simply replace it with the new Notice, adding a few additional statements that reflect more stringent laws protecting mental health information. Note: the additional substance use disorder notice required by 42 CFR §2.22 (the "2.22 Notice") that must accompany the HIPAA Notice of Privacy Practices when providing Part 2 substance use disorder treatment was also written (see Appendix 12).
- **Appendix 10 -- Acknowledgement of Receipt of Notice of Privacy Practices (New)** - The law requires the County to make a good faith effort to obtain written acknowledgement of receipt of the NPP from the patient, or if not received, to document the reason why acknowledgement was not received; this form reflects those requirements that are found in 45 CFR 164.520, and is necessary to document the County's compliance with the requirement so that there is a record that every new patient has in fact been offered a copy of the Notice of Privacy Practices. This form is suitable for use in all County health care programs (public health and behavioral health).
- **Appendix 11 -- Request to Addend Record (New)** - California law gives patients the right to add a statement, up to 250 words in length, to their medical record, and requires health care providers to accept addendums and include them in the patient's "designated record set." This form provides patients the information they need, and the County the documentation it needs, to clearly demonstrate compliance with the law and recognition of this patient right.

- **Appendix 12 -- Part 2 SUD Notice of Privacy Practices (42 CFR §2.22) (New)** -- This new section 2.22 Notice of Privacy Practices was created to be given to all substance use disorder clients, and is necessary to assure compliance with the requirements of Part 2 for use by all County SUD programs. This notice is required in addition to the regular NPP that is given to all County patients/clients/consumers when they first engage in services and whenever the language of either Notice is changed or updated. It also should be freely given to any client upon request, be posted in client areas, and be added to the County behavioral health services/SUD website.
 - **Appendix 13 -- SUD Redislosure Warning (New)** - This document was created to make sure that the “verbatim” warning that must be given per 42 CFR Part 2 §2.32 (a)(2) is used by County SUD programs when information is disclosed pursuant to disclosures made with written consent of the client (it must accompany any information or copies of the SUD record that are sent out at the request of the client).
 - **Appendix 14 -- Business Associate Agreement Checklist (New)** -- This checklist/tool was created, and included after discussion with County risk management and department heads, for use by individual Departments or Programs (as well as by the Office of County Counsel) entering into contracts with vendors or suppliers who need protected health information (PHI) to assist the County or Departments with “operations” -- it includes nineteen (19) items that must be addressed in a BA Agreement or contract, responsibilities of each party, and obligations in the event of a breach; also included with this checklist are copies of actual HIPAA regulations (for reference) and US Code sections outlining the somewhat complex Business Associate requirements that are spread throughout the HIPAA regulations and US Code statutes. Similar to the business associate relationships described in HIPAA, are the related Qualified Service Organization (QSO) and Qualified Service Organization Agreements (QSOA’s) requirements found in 42 CFR Part 2. All of these regulations have been copied and included in the document as a resource: 45 CFR 164.502(e); 45 CFR 164.504(e); 45 CFR 164.308(b); 45 CFR 164.314; 45 CFR 164.410; 42 USC 17932; 42 CFR 2.11; 42 CFR 2.12.
-