Arnall Golden Gregory LLP

Client Alert

Contact Attorney Regarding This Matter:

H. Carol Saul
404.873.8694 – direct
carol.saul@agg.com

Arnall Golden Gregory LLP
Attorneys at Law

171 17th Street NW
Suite 2100
Atlanta, GA 30363-1031

One Biscayne Tower
Suite 2690
2 South Biscayne Boulevard
Miami, FL 33131

2001 Pennsylvania Avenue NW
Suite 250
Washington DC 20006

www.agg.com

OCR / KPMG HIPAA Audit Document Request Revealed: A Useful Tool for HIPAA Self-Assessment

The Office for Civil Rights (OCR) of the Department of Health and Human Services, through its contract with consulting firm KPMG, is currently auditing HIPAA Covered Entities to gauge their levels of compliance with federal privacy and security laws. OCR recently issued its report on the findings for the first twenty auditees, and has stated that the remaining audit targets for 2012 have been notified and asked to provide documentation to KPMG prior to the auditor's site visits. If a Covered Entity has not received notice that it is a 2012 audit target, it is likely "off the hook" for this year. While it is not known exactly what scope or process for HIPAA audits will be rolled out in 2013 and beyond, the document request list being utilized by OCR this year can be used by all Covered Entities, and by Business Associates, as a useful checklist to gauge their level of compliance with HIPAA and prepare for the possibility of future audits. Additionally, since auditees are being given only fifteen days after receipt to provide the requested information, advance work is well-advised.

To date, OCR and KPMG have not published their document request list, but one 2012 auditee has shared its contents with Arnall Golden Gregory. The 37 document and information requests fall into 4 categories: General Information; HIPAA Security (subdivided into administrative, physical and technical safeguards); HIPAA Privacy; and HITECH. Once the omnibus HITECH Act regulations are final, the number of requests under the HITECH category are likely to increase.

Following are the 2012 audit requests.

General Information

- Complete the enclosed "HIPAA Privacy and Security Performance Audit Survey for Selected Covered Entities" (Attachment B) [this attachment asks for general demographic information about the auditee]
- Any previous audit reports, evaluations, or assessments regarding your implementation of HIPAA Privacy and Security Rules and Breach Notification Rule
- Site contact information (name, address, phone number, email address, etc) – KPMG will contact this individual before field work to coordinate field visit
- Please confirm whether your organization uses or discloses PHI in:
  - Fundraising activities; or
  - Research activities

HIPAA Security

- Identify any applicable industry guidance (e.g., studies, practices, regulations, etc…) or other reference material used to develop any of the policies and procedures requested below (NO NEED TO PROVIDE THIS DOCUMENTATION – SIMPLY IDENTIFY)
- Security Officer Contact Information (name, email, phone, address and admin contact info)
- Entity-Level Risk Assessment
- Risk assessments for systems that house ePHI
- Risk Assessment Procedures
- Risk management policy
- Organizational Chart
- Information Security Policies, specifically those documenting security management practices and processes, such as:
  - Access Control
  - Data Protection
  - Acceptable Use
  - Workstation Security
  - Workforce / HR Security
  - Sanction Procedures
- Security Incident Management Plan
- Business Continuity / Disaster Recovery Plan
- Most recent Disaster Recovery Exercise Documentation
- Data backup and recovery procedures
- Physical Security Policies and Procedures
- Data destruction and media reuse procedures
- List of role based access – job level and level of PHI access needed for function; log of employees based on their PHI access type
- Encryption policies and procedures
- Management's internal control / internal audit policies and procedures relative to monitoring IT safeguards
- System-generated user access listing of all individuals with access to systems housing ePHI
- System-generated listing of all new Hires within the past year
- User authentication policies and procedures

HIPAA Privacy

- Identify any applicable industry guidance (e.g., studies, practices, regulations, etc…) or other reference material used to develop any of the policies and procedures requested below (NO NEED TO PROVIDE THIS DOCUMENTATION – SIMPLY IDENTIFY)
- Privacy Officer Contact Information (name, email, phone, address and admin contact info)

- Privacy Policy (s) and Notice of Privacy Practices
- Privacy Practices Documentation, including:
  - Use and Disclosure
  - Right to Request Privacy Information
  - Right to Request Privacy Protection of PHI
  - Access of individuals to PHI
  - Denial of Access to PHI Procedures
  - Amendment of PHI
  - Accounting of Disclosures of PHI
  - Administrative Requirements
- Training documentation for employees over Privacy Practices and organization training policy(s)
- Policies and procedures in place over administrative, technical, and physical safeguards over all forms of PHI
- Complaint handling policies and procedures
- Population of complaints over privacy practices made within the past year (complaint log)
- Sanction and disciplinary policies and procedures over Privacy violations
- Mitigation and disciplinary policies and procedures for when a breach occurs
- Anti-intimidation / anti-retaliation policies and procedures
- Policies and procedures over Uses and Disclosures of PHI, including:
  - Deceased individuals
  - Personal representatives
  - Confidential communication
  - Business associate contract requirements
  - Health plan documentation requirements
  - Treatment, payment, and/or operations
  - Consent and authorization requirements
  - Judicial or administrative proceeding requirements
  - Research requirements
  - Approval or waiver requirements
  - De-identification / re-identification of PHI procedures
  - Restriction of PHI
  - Minimum necessary requirements
  - Limited information provided for fundraising purposes
  - Health care underwriting requirements
  - Identity verification procedures of individuals requesting PHI

HITECH

- Breach notification processes, entity-level risk assessment documentation and capabilities

Regardless of the size or type of your organization, the OCR audit request list can be a critical tool for assessing your state of "audit readiness." Using it to self-evaluate your HIPAA/HITECH compliance status will better prepare you for the possibility of an OCR audit, whether it comes as part of OCR's proactive auditing processes or in response to a self-reported breach, or is triggered by a healthcare consumer's complaint.