



Staying Current with HIPAA

Update on the 2013 revisions effective 9/23/2013

Patient Rights

- Patients may request electronic copies of their records if the information is already maintained in an electronic form. Yale must provide a copy within 30 days.
- Patients (and parents or guardian in the case of minors) can request immunization records be sent directly to schools without signing a HIPAA authorization form.
- We must accept requests from patients who have paid in full for their treatment that the treatment information not be released to their health insurer.

Notice of Privacy Practice – (NOPP)

- Revised NOPP now includes additional required information.
- Revised NOPP or a summary must be prominently posted for patients to see.
- Health Plans must send a revised notice at the time of their next annual mailing.

Decedents

- Health information of individuals who have been deceased for more than 50 years is no longer subject to HIPAA requirements.
- Individuals involved in a patient's care or payment for care prior to death can be allowed access to information.

Breach Reporting

- Unallowable access or disclosure is considered a reportable breach unless a risk assessment determines that there is a low probability that the PHI has been “compromised”.
- We have 60 days to investigate and notify patients.
- Report all incidents immediately to either a supervisor or to a Privacy Officer

Business Associate Agreements

- Clarification that storage of PHI even if it isn't accessed by the vendor creates a BA relationship
- Departments should revisit their current vendors and see if any additional BAAs are needed.

Research

- Record reviews of individuals deceased more than 50 years no longer require authorization or waiver
- Authorizations can be combined for multiple studies, including banking or future unspecified research, as long as:
 - it is clear if any research-related treatments are contingent on signing the RAF and
 - there is a way to authorize the additional uses or activities separately (e.g. check boxes for banking)

Fundraising

- Additional PHI may be disclosed or used for fundraising without a patient authorization including patient demographic data, health insurance status, dates of patient health care services, department of service information, treating physician information, and outcome information such as whether the patient responded well to treatment but not the actual nature of the treatment.
- Added requirement for a clear and easy option to opt-out and we must honor all opt out requests

Marketing and Sale of PHI

- Marketing = receiving money to communicate about a product or service that encourages purchase or use of that product/service. Does not include subsidized prescription reminders.
- Sale = receiving financial remuneration (including in-kind) in exchange for PHI.
- Receiving financial remuneration in exchange for PHI or for marketing activities except in limited circumstances is prohibited without a patient authorization.

Genetic Information Nondiscrimination Act (GINA)

- Prohibition on the use of genetic information for underwriting purposes
- Refers to DNA sequences rather than manifestation of a genetically-based disease

Enforcement

- The Secretary of DHHS is mandated to investigate all reports that suggest a violation arising from willful neglect.
- Penalties include incarceration and fines up to \$1. Million per incident.
- State Attorneys General have authority to investigate
- Can be fines even if we didn't know!

Questions

If you have any questions about HIPAA or the revised HIPAA regulations, feel free to contact the HIPAA Privacy Office at hipaa@yale.edu or call 432-5919