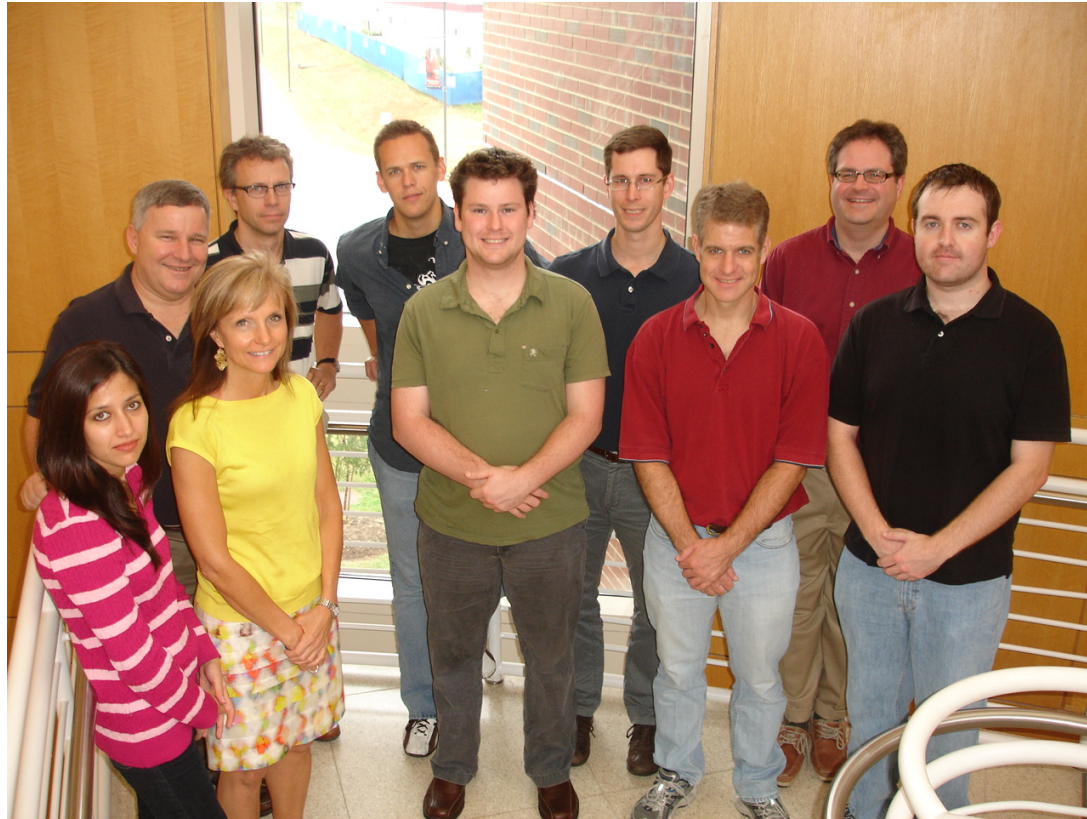


An Analysis of HIPAA Breach Data

Patrick Morrison, Laurie Williams
North Carolina State University
{pjmorris, lawilli3} @ ncsu.edu

^{al}Research - Software Engineering at NCSU

Real Engineers. Real Projects. Real Impact.



<http://www.realsearchgroup.org>

“However beautiful the strategy, you should occasionally look at the results.”

– Winston Churchill

HIPAA Wall of Shame

U.S. Department of Health & Human Services

HHS.gov

Improving the health, safety, and well-being of America

Search

Search

OCR

All HHS

Font Size - +

Print

Download Reader



[HHS Home](#) | [HHS News](#) | [About HHS](#)

Health Information Privacy

[Office for Civil Rights](#)

[Civil Rights](#)

[Health Information Privacy](#)

[OCR Home](#) > [Health Information Privacy](#) > [HIPAA Administrative Simplification Statute and Rules](#) > [Breach Notification Rule](#)

HIPAA

[Understanding HIPAA Privacy](#)

[HIPAA Administrative Simplification Statute and Rules](#)

[Statute](#)

[Privacy Rule](#)

[Security Rule](#)

► [Breach Notification Rule](#)

[Other Administrative Simplification Rules](#)

[Enforcement Rule](#)

[Combined Text of All Rules](#)

[Enforcement Activities & Results](#)

[How to File a Complaint](#)

[News Archive](#)

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Full DataSet [CSV format \(18 KB\)](#) [XML format \(57 KB\)](#)

Select a column head to sort by that column. Select again to reverse the sort order. Select an individual record to display it in full below the table.

Filter: 479 records showing

Name of Covered Entity	State	Individuals Affected	Date of Breach	Type of Breach	Location of Breached Info
Accendo	AZ	175,350	2011-01-01	Unauthorized Access/Disclosure	Paper
Access Medical Group	PR	7,606	2012-01-11	Theft	Laptop
Adult & Child Care Center	IN	550	2012-05-10	Hacking/IT Incident	Other

Example...

- “Protected health information was released from the covered entity when an imposter, posing as representatives of the legitimate recycling service used by the covered entity, removed several barrels of purged x-ray films and film jackets.”

Breach Fields Reported

- **Name of Covered Entity**
- **State**
- **Individuals Affected**
- **Date of Breach (Posted or Updated)**
- **Type of Breach**
- **Location of Breached Info**
- **Summary**

Three Fields Considered

- Breach Type

- e.g. 'Theft', 'Loss', 'Hacking/IT Incident'

- Breach Location

- e.g. 'Laptop', 'Email', 'Backup tape'

- Breach Summary

- Text description of breach (102 summaries/392 records)

Results Table

Breach Count Type/Location	Theft	Unauthorized Access/Disclosure	Loss	Hacking/ IT Incident	Improper Disposal	Unknown	Other	
Paper	27	46	13		20	2	1	109
Laptop	87	5	4	1				97
Computer	51	10	4	10		1		76
Other Portable Electronic Device	40	2	25			1		68
Network Server	16	18	1	21	1			57
Other	4	7	11			1	1	24
Email	2	6		2				10
Electronic Medical Record		4		1		1		8
X-ray film	3				2			5
Backup tape	1		3					4
Compact Disc	1		1					2
Hard drive	1							
Total	235	98	62	35	23	6	2	461

Results Summary

- Theft, Loss, and Improper Disposal, combined, account for almost 70% of breach instances $((235+62+23)/461)$.
- The most common media breached across Types was Paper, with 24% of breach instances (109/461).
- Encryption is almost non-existent in reported breach instances.

Recommendations

- Disable the print button
- Encrypt PHI at its creation
 - (and decrypt only for use)
- Limit data on portable devices

Concerns...

- A reviewer observed that our recommendations were not novel; we agree.
- It appears that these ideas are not yet universally implemented.
- **Consider the entire workflow, not just the software.**

Surely there's more we can do...

- How do we translate what is known about security and privacy in to health care practice?
- Can we reshape the health care workflow through software design?
 - Can 'The Cloud' help limit the number of copies of PHI?
 - Could we encrypt what's printed, and have providers wear 'Decoder glasses'?
 - Your input is clearly needed here...

Thank You