



**CMS 2010 BI-REGIONAL MEDICARE HEALTH PLAN COMPLIANCE
CONFERENCE**
Boston & New York – Serving Our Beneficiaries Together

Verbatim Transcript
Privacy and Security – Office for Civil Rights
Frank Winter, Lisa Lee Anderson, J.D., and Kelli Robinson

>> GOOD AFTERNOON, EVERYONE.

>> GOOD AFTERNOON.

>> WE ARE HERE TO LEARN
A LITTLE BIT ABOUT HIPAA AND,

YOU KNOW, PRIVACY.

I ALWAYS LOOK
AT THE WORD HIPAA

AND I THINK THERE SHOULD
BE A "P" IN THERE.

I'M ALWAYS,
"ARE THERE 2 Ps?"

"IS THERE ONE P?"

YOU KNOW, AND IF
THERE WAS ANOTHER "P",

I THINK IT WOULD
BE FOR PRIVACY

BECAUSE THAT'S A LOT
OF WHAT HIPAA IS ABOUT.

AND IN OUR AGENCY--I'M WITH--
MY NAME'S FRANK WINTER,

I'M WITH THE CMS REGIONAL
OFFICE HERE IN NEW YORK.

AND WE KNOW THAT AS WE PUSH
HEALTHCARE PROVIDERS TO ADOPT

ELECTRONIC HEALTH RECORDS
AND ALSO FOR PAYERS TO WORK

WITH THEM TO DO SO,

THE NUMBER ONE CONCERN
THAT THE PUBLIC

HAS ABOUT ELECTRONIC
HEALTH RECORDS

IS PRIVACY AND SECURITY.

AND THAT'S WHAT REALLY
HIPAA IS ALL ABOUT.

AND SO WE HAVE 2 DISTINGUISHED
SPEAKERS HERE FROM THE OFFICE

OF CIVIL RIGHTS OF HHS WHO
ARE GOING TO TALK ABOUT HIPAA.

AND ERIC BROWN
IS GOING TO START.

HE'S SUPERVISORY EQUAL
OPPORTUNITY SPECIALIST AT OCR

AND HE'S GOING TO BE JOINED
ALSO BY KELLI ROBINSON,

WHO IS THE SECURITY RULE LEAD
AT THE OFFICE OF CIVIL RIGHTS.

AND THEY'RE BOTH
INVESTIGATORS, THEY HAVE

A ROLE IN COMPLIANCE,

AND THEY'RE EXPERTS
IN THIS AREA.

ERIC IS GOING TO TALK
ABOUT PRIVACY BREACH

AND NOTIFICATION, AND
KELLI WILL BE TALKING

ABOUT THE SECURITY RULE.

SO WITH THAT, I WILL LEAVE
IT TO ERIC TO START OFF.

AND WE WILL HAVE ABOUT
10 MINUTES AT THE END

OF THE SESSION FOR QUESTIONS.

WE DO ASK IF YOU CAN THAT
IF YOU HOLD YOUR QUESTIONS

UNTIL THE END. THANK YOU.

>> GOOD AFTERNOON, AGAIN.

THANKS FOR COMING.

I'D JUST LIKE
TO TAKE A QUICK POLL

AS TO HOW MANY OF YOU
IN THE ROOM

ARE COMPLIANCE OFFICERS OR
PRIVACY SECURITY OFFICERS?

OK, BECAUSE WE WERE INFORMED,

WHEN WE WERE ASKED
TO DO THIS PRESENTATION

THAT THIS SHOULD
BE A HIPAA 101 TYPE REVIEW.

AND I DON'T WANT TO BORE SOME
OF YOU WHO'VE HAD AD NAUSEA,

YOU KNOW, HIPAA TRAINING.

SO I SEE MAYBE ABOUT 5 HANDS
OR 6 HANDS OF INDIVIDUALS

WHO ARE COMPLIANCE OFFICERS,

OR PRIVACY,
OR SECURITY OFFICERS.

SO WHAT I'LL DO IS I'LL GO
THROUGH THE FUNDAMENTALS

FOR THE REST OF YOU, AND FOR
THOSE WHO'VE ALREADY BEEN

THROUGH THIS, WHAT YOU CAN
DO IS TAKE THIS OPPORTUNITY

TO WRITE DOWN SOME QUESTIONS
THAT YOU MIGHT HAVE THAT'S MORE

ADVANCED THAN THE INFORMATION
THAT YOU MAY SEE HERE.

WE HAVE A POWER POINT
PRESENTATION AND WE'LL JUST GO

THROUGH SOME OF THE ELEMENTARY
FACETS OF THE PRIVACY RULE

FIRST, AND THEN AFTER WE DO
THE PRIVACY RULE, WE'LL TALK

ABOUT THE SECURITY RULE,
AND THEN WE'LL TALK

ABOUT THE BREACH
IN NOTIFICATION RULE,

WHICH APPLIES TO BOTH
PRIVACY AND SECURITY.

ALL RIGHT.

THE KEY ELEMENTS OF THE
PRIVACY RULE, AS YOU CAN SEE,

YOU KNOW,
WHO DOES IT APPLY TO?

AND THAT'S THE COVERED ENTITY.

WHAT INFORMATION THAT'S
TRYING TO BE PROTECTED?

AND WE CALL THAT PROTECTED
HEALTH INFORMATION AND WE'LL

FURTHER DEFINE THAT AS WE GO.

WHAT TYPE OF PROTECTED
HEALTH INFORMATION AND

IN WHAT CAPACITY?

WE'RE TALKING ABOUT USES
AND DISCLOSURES OF PROTECTED

HEALTH INFORMATION,
INDIVIDUAL RIGHTS WITH RESPECT

TO THE PRIVACY RULE.

WHAT RIGHTS PATIENTS
AND INSUREDS HAVE.

THE ADMINISTRATIVE
REQUIREMENTS--THOSE ARE

THE OBLIGATIONS
OF THE COVERED ENTITIES

WITH RESPECT
TO THE PRIVACY RULE.

AND THEN THE COMPLIANCE AND
ENFORCEMENT PIECE--WHAT WE DO

ONCE THERE'S BEEN
A POSSIBLE BREACH

OR VIOLATION OF THE RULE.

THE HIPAA STANDARDS APPLY,
YOU KNOW,

ONLY TO COVERED ENTITIES,

AND COVERED ENTITIES
IN THE RULE

IS DEFINED AS
HEALTH CARE PROVIDERS

WHO TRANSMIT
ANY HEALTH INFORMATION

IN ELECTRONIC FORM
IN CONNECTION

WITH A TRANSACTION
CONTEMPLATED

BY THE SECRETARY
OF HHS IN THE RULE,

HEALTH PLANS, AND HEALTH CARE
CLEARING HOUSES.

NEXT. PROTECTED HEALTH
INFORMATION IS DEFINED

AS INDIVIDUALLY IDENTIFIABLE
HEALTH INFORMATION,

AND I ALLUDED
TO THIS EARLIER

DURING THE PLENARY SESSION
THAT THAT'S INFORMATION

SUCH AS A PERSON'S NAME,
SOCIAL SECURITY NUMBER,

DATE OF BIRTH--ALL THAT
INFORMATION THAT ONE WOULD

NORMALLY DE-IDENTIFY WHEN
THEY'RE ENGAGING IN RESEARCH.

THE INFORMATION ALSO HAS TO
BE TRANSMITTED OR MAINTAINED

IN ANY FORM OR MEDIUM
BY THE COVERED ENTITY

OR BUSINESS ASSOCIATE.
UM...NEXT SLIDE.

INDIVIDUALLY IDENTIFIABLE

HEALTH INFORMATION--

AND WE ALREADY
TALKED ABOUT THIS--

IT'S CREATED OR RECEIVED
BY THE COVERED ENTITY.

AND I TALKED ABOUT EARLIER
ABOUT THE DESIGNATED RECORD

SET, AND WE'LL GET INTO THAT,

BUT IT RELATES
TO THE INDIVIDUAL'S

PHYSICAL OR MENTAL HEALTH,
OR THE PROVISION OF,

OR PAYMENT FOR HEALTH CARE,

AND IT IDENTIFIES
THE INDIVIDUALS REASONABLY

AND SUFFICIENTLY ENOUGH
WHEREIN ONE CAN, YOU KNOW, DO

THEIR OWN
PRELIMINARY INVESTIGATION

AND DETERMINE
WHO THE INDIVIDUAL IS.

AND I'LL GIVE YOU JUST
A BRIEF SITUATION

THAT WE HAD
IN THE OFFICE.

WE RECEIVED A COMPLAINT
WHERE A PHYSICIAN--

A SMALL PRACTITIONER--WAS
SPEAKING TO A PATIENT

WHO HE WAS TREATING
AND THE PATIENT INDICATED

THAT HE WAS
A PROFESSIONAL GAMBLER.

AND THE PHYSICIAN SAID,
"OH, THAT'S INTERESTING.

"I HAVE ANOTHER PATIENT
WHO'S A PROFESSIONAL GAMBLER.

"HE'S BEEN ON TELEVISION
AND THE POKER THAT THEY DO

"ON, I THINK, ESPN,
OR SOMETHING LIKE THAT.

HE'S, YOU KNOW, QUITE
SKILLED AT WHAT HE DOES."

NOW, THIS PHYSICIAN
AND THIS PATIENT COMES

FROM A VERY SMALL TOWN,

AND SO THERE WEREN'T THAT
MANY PROFESSIONAL GAMBLERS

IN THE TOWN.

AND SO THE PATIENT WAS
EASILY ABLE TO IDENTIFY

WHO THE PHYSICIAN
WAS REFERRING TO,

AND THE PHYSICIAN HAD GONE
ON TO TALK ABOUT

THIS PATIENT'S PHI,
AND THE PATIENT

THAT HE WAS SEEING SENT
IN A COMPLAINT TO US,

YOU KNOW, ON BEHALF OF THE
OTHER PROFESSIONAL GAMBLER.

AND SO THE QUESTION WAS,
YOU KNOW, WHETHER OR NOT,

YOU KNOW, THERE WAS
A BASELINE OF INFORMATION

TO ACCEPT THIS AS A VIABLE
COMPLAINT AND INVESTIGATE.

AND SO WE HAD TO LOOK AT
THE DEFINITION OF INDIVIDUALLY

IDENTIFIABLE
HEALTH INFORMATION.

SO, YOU KNOW, SOMETIMES
YOU LOOK AT THIS STUFF

AND YOU SAY, "OH,
THIS IS SO MUNDANE.

IT REALLY DOESN'T MEAN ANYTHING,
ALL THESE DEFINITIONS."

BUT THAT'S AN INSTANCE
WHERE IT ACTUALLY MATTERED

AS TO WHETHER OR NOT
WE WOULD ACCEPT

A COMPLAINT
FOR INVESTIGATION.

AND, ACTUALLY, WE DID.

SO I JUST WANTED
TO RELAY THAT TO YOU

THAT THE DEFINITIONS
MEAN SOMETHING.

NEXT SLIDE.

THE GENERAL RULE AROUND HIPAA
IS THAT COVERED ENTITIES MAY

NOT USE OR DISCLOSE PHI,
EXCEPT THAT AS PERMITTED

OR REQUIRED
BY THE PRIVACY RULE.

AND THE PRIVACY RULE ONLY
REQUIRES THE DISCLOSURE

OF PROTECTED HEALTH

INFORMATION IN 2 INSTANCES,

AND THAT'S IF THE INDIVIDUAL
REQUESTS ACCESS TO THEIR PHI

OR INFORMATION ABOUT THEIR
HEALTH, OR TO THE DEPARTMENT

OF HSS--IF THE SECRETARY,
MEANING US--IF WE OR ANY OTHER

FACET OF HSS IS PURSUING AN
INVESTIGATION AND THEY REQUEST

INFORMATION PURSUANT TO A
PRIVACY RULE OR SECURITY RULE

MATTER, THAT INFORMATION
HAS TO BE DISCLOSED TO US,

OR MADE AVAILABLE TO US.

THAT'S SOMETHING THAT ALL
TOO OFTEN CONFUSES COMPLIANCE

OFFICERS AND PRIVACY
OFFICERS AND SECURITY OFFICERS.

FREQUENTLY, IT COMES UP IN THE
CONTEXT WHEREIN A PATIENT WILL

REQUEST ACCESS
TO THEIR INFORMATION

AND THE PATIENT MAY SAY,
"I WANT YOU TO SEND ME A COPY

"OF MY MEDICAL RECORDS
IN CARE OF MY REPRESENTATIVE

MY ATTORNEY."

AND COMPLIANCE OFFICERS WILL
GET THAT REQUEST AND SAY,

"NO, WE'RE NOT GIVING YOU
ACCESS TO THIS INFORMATION.

"WE DON'T HAVE TO SEND
IT TO YOUR LAWYER.

WE ONLY HAVE TO
GIVE IT TO YOU."

WELL, IF THE PATIENT REQUESTS
THE INFORMATION TO HIMSELF

IN CARE OF SOMEONE ELSE
AT SOMEONE ELSE'S ADDRESS,

YOU HAVE TO PROVIDE THAT
INFORMATION TO THE PATIENT.

THAT'S A REQUIRED DISCLOSURE.

THE FLIPSIDE OF THAT,
SOMETIMES WE'LL HAVE PATIENTS

WHO SAY THAT, "YOU KNOW,

"I'VE BEEN IN
AN AUTOMOBILE ACCIDENT.

"I NEED MY RECORDS
AND I REQUESTED THEM

"FROM MY PHYSICIAN
AND THE PHYSICIAN REFUSES

TO GIVE ME
MY RECORDS."

SINCE WHAT WE HAVE TO ASK IS,

"WELL, HOW DID YOU MAKE
THE REQUEST?

"DID YOU DO IT IN WRITING?

IF YOU DID SO, PROVIDE US
A COPY OF THE WRITING."

AND WE'LL SEE OFTENTIMES,
TOO, THEY'LL SEND US A COPY

OF A LETTER THAT THE ATTORNEY
SENT TO THE HEALTH CARE

PROVIDER ASKING FOR ACCESS
TO ALL AND ANY MEDICAL RECORDS

THAT WERE GENERATED
AS A RESULT OF THE ACCIDENT.

AND THE COVERED ENTITIES,
YOU KNOW, MUCH TO YOUR CREDIT,

REFUSES TO SEND THE RECORDS,
AND SO THE PATIENT FILES

A COMPLAINT WITH US, AND WE
HAVE TO TAKE THAT OPPORTUNITY

TO EDUCATE THE PATIENT AND
THE PUBLIC THAT THOSE ARE NOT

REQUIRED DISCLOSURES, AND
SO WE TELL THEM HOW TO MAKE

THE REQUEST. SO I JUST
WANTED TO POINT THAT OUT.

UM...WE HAD ANOTHER SLIDE.

OK. PERMITTED USES
AND DISCLOSURES.

I GUESS IT'S COMING UP
A LITTLE SLOWER.

UM...THE PERMITTED USES
AND DISCLOSURES ARE THOSE

DISCLOSURES WHERE THE COVERED
ENTITY DOES NOT HAVE TO HAVE

THE CONSENT, WE LIKE
TO SAY IS THE RULE--

THE TERMS THE RULE USES--THE
AUTHORIZATION OF THE PATIENT

IN ORDER TO DISCLOSE THE
PATIENT'S HEALTH INFORMATION.

SO, MEANING THAT THE RULE
ACTUALLY IDENTIFIES THOSE

INSTANCES WHERE A HOSPITAL
OR DOCTOR'S OFFICE CAN,

WITHOUT THE PATIENT'S
AUTHORIZATION OR CONSENT,

DISCLOSE
THE HEALTH INFORMATION.

AND THAT'S, HONESTLY, TO
THE PATIENT HIM OR HERSELF.

YOU DON'T NEED THEIR CONSENT
TO DISCLOSE INFORMATION

TO THEM FOR PURPOSES OF
TREATMENT, PAYMENT, OR HEALTH

CARE OPERATIONS--AND WE'LL
DISCUSS THAT IN A LITTLE

GREATER DETAIL.
AND IN THOSE INSTANCES

WHERE THE PATIENT
DOESN'T HAVE TO BE

GIVEN AN OPPORTUNITY
TO AGREE OR OBJECT.

AND I'LL JUST GIVE YOU
A QUICK EXAMPLE OF THAT.

THE SITUATION WHERE A PATIENT
IS TAKEN TO THE EMERGENCY ROOM

AND THE HOSPITAL
HAS A FACILITY DIRECTORY,

AND THEY PUT IN THERE JUST BASIC
INFORMATION ABOUT, YOU KNOW,

THE PATIENT WAS BROUGHT IN,

THE PATIENT WAS
SENT TO EMERGENCY,

AND THE PATIENT IS STABLE.

SOMETHING TO THAT EFFECT.

WELL, THE HOSPITAL JURY

HAS TO GIVE THE PATIENT

AN OPPORTUNITY TO REJECT
FROM BEING A PART

OF THE FACILITY DIRECTORY.

OFTENTIMES, IT'S NOT SOMETHING
JUST DIRECT, IT'S USUALLY

ON SOME SORT OF FORM ASKING,
DO YOU WANT TO BE EXCUSED

FROM OR EXEMPTED
FROM THE FACILITY DIRECTORY?

MOST PATIENTS PROBABLY
ARE NOT AWARE OF IT.

AND SO THAT INFORMATION IS
IN THE FACILITY DIRECTORY.

AND THAT'S HOW YOU GET,
YOU KNOW, REPORTERS AND OTHER

INDIVIDUALS WHO CALL,
THE POLICE OR FAMILY MEMBERS

WHO ARE LOOKING
FOR SOMEONE TO FIND OUT

IF THEY'RE
IN THE HOSPITAL.

BECAUSE YOU CAN ACTUALLY GET
THAT INFORMATION--JUST THAT

BASIC INFORMATION--FROM
THE FACILITY DIRECTORY.

AND THAT'S A SITUATION
WHERE YOU HAVE THE PATIENT

WHO MAY NOT BE GIVEN
AN OPPORTUNITY TO AGREE

OR OBJECT BECAUSE I
PREFACED THIS SCENARIO

WITH THAT THE PATIENT IS

IN THE EMERGENCY DEPARTMENT.

NOW IF THE PATIENT CAME
IN ON HIS OR HER OWN,

THEY WOULD HAVE TO HAVE THAT
OPPORTUNITY TO AGREE OR OBJECT.

BUT OFTENTIMES WHEN YOU COME
IN THROUGH THE EMERGENCY

DEPARTMENT, YOU MAY NOT BE
IN A POSITION TO DO THAT.

SO I JUST WANTED
TO POINT THAT OUT.

>> DOES IT MATTER IF IT'S
AN OPT IN OR OPT OUT?

>> CAN YOU CLARIFY WHAT YOU
MEAN BY OPT IN OR OPT OUT?

WELL, THE PATIENT HAS TO
BE GIVEN THAT OPPORTUNITY.

SO, UM...

WHATEVER FORM OR MEDIUM
YOU PROVIDED TO THE PATIENT,

IF IT'S A SITUATION WHERE IF
YOU DON'T SIGN THIS,

THEN YOU AUTOMATICALLY
INCLUDE IT,

THAT'S ALL THE RULE REQUIRES.

IT DOESN'T REQUIRE
SOME PROACTIVE, YOU KNOW,

UM, YOU KNOW, UM,
ACTION ON YOUR PART.

OK. NEXT SLIDE.

COMPLAINTS
TO THE COVERED ENTITY.

THE COVERED ENTITY MUST HAVE
A PROCESS FOR INDIVIDUALS

TO MAKE COMPLAINTS CONCERNING
THEIR PRIVACY POLICIES

AND PROCEDURES.

AND I ALLUDED TO THIS
IN THE EARLIER SESSION.

NO PROVISIONS ON HOW
THE COVERED ENTITIES

COMPLAINT PROCESSES
MUST OPERATE.

WHAT THAT MEANS IS THAT
THE RULE DOESN'T TELL YOU

HOW TO CONSTITUTE
YOUR COMPLAINT PROCESS.

THE ONLY THING THE RULE SAYS
IS THAT YOU MUST DOCUMENT

COMPLAINTS, AND YOU MUST
DOCUMENT THEIR DISPOSITION.

AND SO THIS IS ANOTHER SECTION

THAT'S RIPE FOR SOMETIMES
CONFUSION FOR COVERED ENTITIES.

UM, UM,
YOU'LL HAVE SITUATIONS

WHERE THE COVERED
ENTITY BELIEVES

THAT THEY'RE OBLIGATED
TO PROVIDE THE COMPLAINANT

OR THE PATIENT, HIM OR HERSELF,

WITH A FULL SUMMARY OF
THEIR INTERNAL INVESTIGATION

WITH REGARDS TO A COMPLAINT THAT
THEY MAY HAVE LOOKED INTO.

OR THE PATIENT MAY THINK
THAT THEY'RE ENTITLED

TO HAVE THE RESULTS
OF AN INVESTIGATION

THAT DERIVED FROM A COMPLAINT
THAT THEY FILED.

AND OFTENTIMES, WE TAKE THAT
OPPORTUNITY TO DO TECHNICAL

ASSISTANCE WITH THE COVERED
ENTITY, AS WELL AS PROVIDE

EDUCATION TO THE PATIENT AND
THE PUBLIC, TO LET THEM KNOW

THAT THE RULE ONLY REQUIRES
2 THINGS WITH RESPECT

TO THE COMPLAINT PROCESS, AND
THAT'S THAT THEY BE DOCUMENTED

AND THEN THE DISPOSITION
ALSO BE RECORDED SOMEHOW.

THAT'S IT. YOU DON'T
HAVE A RIGHT TO FIND OUT

WHAT THE RESULTS
OF THAT INVESTIGATION IS,

AND THAT'S USUALLY
WHAT PATIENTS WANT.

HAVING SAID THAT, IT MAKES,
YOU KNOW, GOOD CUSTOMER SERVICE

TO FOLLOW UP WITH THE PATIENT,

TO LET THEM KNOW, YOU KNOW,
WHAT WAS THE OUTCOME.

YOU DON'T HAVE TO GIVE
THEM ALL THE DETAILS THAT,

YOU KNOW, THE EMPLOYEE
WAS DISCIPLINED,

OR THE EMPLOYEE
WAS TERMINATED

OR--YOU DON'T HAVE
TO SAY ALL THAT.

YOU CAN JUST LET THEM KNOW,
YEAH, YOUR COMPLAINT WAS

SUBSTANTIATED AND WE TOOK
THE APPROPRIATE, YOU KNOW,

ACTION THAT WE THOUGHT,
YOU KNOW, WAS NECESSARY

IN THIS CASE.

I THINK SOME PATIENTS
WILL BE HAPPY WITH THAT.

NOT ALL, BUT I THINK
SOME WILL BE HAPPY

IN THAT KNOWING THAT
THEY WERE RIGHT ALL ALONG

WHEN THEY
FILED THEIR COMPLAINT.

THAT THEY WERE WRONG
AND YOU ACKNOWLEDGED

THAT THEY WERE WRONG.

WHAT HAPPENS WITH US
IS WE GET THE COMPLAINT

BECAUSE THEY'RE
LEFT IN LIMBO.

SO, YOU KNOW, YOUR HOSPITAL
OR THE COVERED ENTITY

DOESN'T GET BACK TO THEM
TO LET THEM KNOW ANYTHING

ONE WAY OR THE OTHER, AND SO
THEY'RE CALLING AND CALLING,

AND NO ONE'S
SAYING ANYTHING.

SO, "ALL RIGHT, THEN, I'M
GOING TO FILE A COMPLAINT."

SO WE COULD MINIMIZE SOME
OF THESE INVESTIGATIONS

IF YOU JUST GET BACK TO THEM.

THE RULE ALSO TALKS ABOUT,
YOU KNOW, FOR PURPOSES

OF THE COMPLAINT PROCESS, THIS
IS PART AND PARCEL OF IT.

IT'S NOT IN THE SAME SECTION,

BUT IT'S UNDER THE
ADMINISTRATIVE REQUIREMENTS

THAT EACH COVERED ENTITY
HAS TO DESIGNATE

AN OFFICIAL
TO ACCEPT THE COMPLAINTS.

AND THAT'S USUALLY
THE PRIVACY OFFICER.

AND THEN IN YOUR NOTICE
OF PRIVACY PRACTICE

YOU HAVE TO
INDICATE WHO THAT PERSON IS

AND HOW THAT PERSON
CAN BE REACHED.

SOMETIMES WHEN WE HAVE
INVESTIGATIONS CONCERNING

THE NOTICE OF PRIVACY PRACTICES,

WE'LL SEE THAT THERE LIES
THE PROBLEM.

UM, INDIVIDUALS OR PATIENTS
DON'T KNOW WHO TO COMPLAIN TO

BECAUSE THAT WAS NOT INCLUDED
IN YOUR NOTICE OF PRIVACY

PRACTICE, AND THAT HAS TO
BE INCLUDED IN YOUR NOTICE

OF PRIVACY PRACTICE
AS PART

OF THE
ADMINISTRATIVE REQUIREMENTS.

THAT GOES HAND IN HAND
WITH YOUR COMPLAINT PROCESS.

YOU HAVE TO DESIGNATE
THE PRIVACY OFFICIAL.

AND 9 TIMES OUT OF 10, THAT'S
THE CASE, BUT THEN YOU DON'T

PROVIDE THAT INFORMATION
TO THE PUBLIC IN YOUR NOTICE

OF PRIVACY PRACTICE AND HOW
THAT PERSON CAN BE REACHED.

NOW WHAT WE HAVE SEEN,
AND THIS SEEMS TO BE PRETTY

MUCH A PRACTICE
WITH COVERED ENTITIES,

AND WE DON'T
OBJECT TO IT,

IS THAT YOU MAY NOT IDENTIFY
WITH ANY SPECIFICITY

THE NAME OF THE INDIVIDUAL

AND THE INDIVIDUAL'S
CONTACT INFORMATION.

THAT'S OK.

TO SAVE YOURSELF ON SOME
RESOURCES BECAUSE THERE'S

A LOT OF TURNOVER,
YOU CAN JUST INDICATE

THAT THE DESIGNATED
PRIVACY OFFICIAL

WILL BE THE VICE PRESIDENT
OF COMPLIANCE,

AND THAT PERSON CAN BE
REACHED AT--AND YOU CAN

JUST GIVE
THE GENERAL HOSPITAL NUMBER

OR MAILBOX WHERE
COMPLAINTS GO.

YEAH, AGAIN, THAT DOESN'T HAVE
THE DETAIL OR SPECIFICITY

THAT MAYBE SOME
INDIVIDUALS WOULD LIKE,

BUT THAT
SATISFIES THE RULE.

>> POLICIES AND PROCEDURES--
THAT'S THE BIG, YOU KNOW,

TO-DO WITH RESPECT
TO THE PRIVACY RULE.

THAT'S THE FIRST THING
A COVERED ENTITY SHOULD HAVE

DONE IN 2003 OR PRIOR
TO 2003 WAS CREATE POLICIES

AND PROCEDURES FOR ALL OF
THE ADMINISTRATIVE REQUIREMENTS

IN THE RULE INFO.

ALL OF THOSE SECTIONS
OF THE RULE THAT YOU MUST

COMPLY WITH.

AND THAT'S YOUR USES

AND DISCLOSURE SECTIONS,

YOUR SAFEGUARD SECTIONS,
YOUR INDIVIDUAL RIGHTS

SECTIONS WHICH TALKS ABOUT,
YOU KNOW, A PATIENT HAVING

THE RIGHT TO ACCESS
TO THEIR PHI, OR THEY REQUEST

AN ACCOUNTING OF DISCLOSURES,
OR AN AMENDMENT.

YOU HAVE TO HAVE RULES
FOR THOSE PARTICULAR SECTIONS

IN THE PRIVACY RULE.

AND WE FIND, YOU KNOW,
UNFORTUNATELY, FREQUENTLY,

THAT, YEAH, COVERED ENTITIES
DON'T HAVE RULES, OR POLICIES

AND PROCEDURES, FOR THOSE
PARTICULAR SECTIONS.

THEY JUST HAVE THIS GENERAL
RULE ON POLICY THAT TALKS ABOUT,

YOU KNOW, THE CONFIDENTIALITY
OF PATIENT HEALTH INFORMATION,

OR THE PRIVACY OF PATIENT
HEALTH INFORMATION,

BUT THERE'S NOT THE DETAILS
OR SPECIFICITY WITH RESPECT

TO EACH OF THOSE SECTIONS,
THOSE INDIVIDUAL'S RIGHTS

SECTION,
THE SAFEGUARD SECTIONS,

OR THE ADMINISTRATION
REQUIREMENT SECTIONS,

AND YOU HAVE TO DO THAT.

UM, ANOTHER THING WITH RESPECT
TO THE POLICIES AND PROCEDURES

IS THAT ANY TIME THERE'S A
MATERIAL CHANGE, A SUBSTANTIAL

CHANGE TO THE POLICIES
AND PROCEDURES,

THEN YOU HAVE TO
PUT OUT A NEW NOTICE

OF PRIVACY PRACTICE,
OR YOU HAVE

TO PROVIDE MORE TRAINING
TO YOUR STAFF WITH RESPECT

TO THE MATERIAL CHANGES
TO YOUR POLICIES AND PROCEDURES.

THAT HAPPENS AS WELL.

YOU KNOW, IT'S A CRACK
IN THE SYSTEM, WE FIND,

THAT THERE'LL BE A MAJOR CHANGE
TO THE POLICIES AND PROCEDURES,

BUT NO TRAINING FOR THE STAFF.

AND THE RULE REQUIRES THAT ANY
TIME YOU HAVE MATERIAL CHANGES,

YOU HAVE TO PROVIDE
TRAINING TO THE STAFF.

AND EVEN IF YOU JUST REVISE
THE POLICIES AND PROCEDURES,

THAT COULD BE CONSIDERED
A MATERIAL CHANGE,

OR SUBSTANTIAL CHANGE WHERE
TRAINING NEEDED TO BE PROVIDED.

SAFEGUARDS AND MITIGATION--
WHAT WE FIND DURING THE COURSE

OF OUR INVESTIGATIONS,
THE RULE STATES THAT YOU HAVE

IMPLEMENT APPROPRIATE
ADMINISTRATIVE PHYSICAL

AND TECHNICAL SAFEGUARDS
TO PROTECT THE PRIVACY OF PHI.

AND THEN YOU HAVE TO MITIGATE
ANY HARMFUL EFFECT OF A USE

OR DISCLOSURE OF PHI, WHICH IS
KNOWN TO THE COVERED ENTITY

TO THE EXTENT THAT,
YOU KNOW, THAT'S PRACTICAL.

WITH RESPECT TO THIS SECTION
OF THE RULE, WE FIND THAT YOU

MAY HAVE SAFEGUARDS IN PLACE,
AND SOMETIMES, YOU KNOW,

THE BEST SAFEGUARDS IS NOT
GOING TO PREVENT A DISCLOSURE

BECAUSE IT'S ONLY AS GOOD

AS THE STAFF IN IMPLEMENTING
THOSE SAFEGUARDS.

BUT WHAT WE FIND IS THAT
YOU'LL HAVE THE POLICIES

AND PROCEDURES, YOU'LL HAVE
THE SAFEGUARDS IN PLACE,

THERE'LL BE A POSSIBLE BREACH,
AND YOU MAY EVEN SUBSTANTIATE

THAT THERE WAS A POSSIBLE
BREACH, BUT YOU FORGET TO DO

THE OTHER PIECE TO THIS,
AND THAT'S TO MITIGATE ANY

HARMFUL EFFECT
THAT YOU ARE AWARE OF

TO THE EXTENT PRACTICABLE.

AND THAT'S WHERE
WE THEN GET YOU.

AND, AS I SAID EARLIER, THIS IS
REALLY NOT A "GOT YOU" GAME,

BUT WE HAVE TO MAKE
SURE THAT, YOU KNOW,

YOU'RE COMPLYING WITH ALL
FACETS OF THE RULE.

SO, YOU KNOW, YOU'RE
REALLY DOING A DISSERVICE

TO YOURSELF, TO CREATE THESE
POLICIES, TO TRAIN YOUR STAFF,

TO IMPLEMENT THESE SAFEGUARDS,

AND THEN WHEN
SOMETHING HAPPENS,

YOU DON'T TAKE
THE NECESSARY ACTION

TO MITIGATE THE HARM.

AND I'LL JUST GIVE YOU
A QUICK EXAMPLE OF THAT

IS WE'RE IN SOMETHING
THAT I SAID EARLIER TODAY,

WHERE IF A PATIENT
COMES TO YOU

AND ASKS FOR A DOCTOR'S NOTE

BECAUSE THEY WAS OUT SICK,

AND, YOU KNOW, YOU WERE SEEING
THAT AT YOUR OFFICE

AND YOU PROVIDED THEM
WITH SERVICE,

OR AT THE HOSPITAL,

AND ACTUALLY TO SEND

A DOCTOR'S NOTE, YOU SEND
THE DOCTOR'S NOTE OVER AGAIN,

YOU DISCLOSE
TOO MUCH INFORMATION,

MORE THAN THE MINIMALLY
NECESSARY AMOUNT OF INFORMATION.

AND THEN THE PATIENT
COMPLAINS TO YOU,

AND THEN YOU SAY,
YOU KNOW, "I'M SORRY."

IN SOME INSTANCES, THAT MIGHT
BE ENOUGH TO SEND A LETTER

OF APOLOGY TO THE PATIENT,
BUT THEN THERE'S OTHER

INSTANCES WHERE YOU MIGHT
BE ABLE TO DO MORE

TO MITIGATE THE HARM.

UM, AND WHAT YOU NEED TO DO
AS COMPLIANCE OFFICERS

AND PRIVACY OFFICERS, IS TO
INVESTIGATE, TO SEE--AND THAT

MIGHT MEAN SPEAKING
TO THE PATIENT.

YOU KNOW, IS THERE ANYTHING
ELSE THAT WE CAN DO, YOU KNOW,

BECAUSE, YOU KNOW,
WE SENT TOO MUCH INFORMATION

AND, YOU KNOW,
YOUR EMPLOYER KNOWS

THAT YOU HAVE THIS
PARTICULAR ILLNESS?

I DON'T KNOW.

IT'S GOING TO BE DETERMINED
ON A CASE-BY-CASE BASIS.

BUT THAT'S
A CRITICAL PIECE TO THIS.

YOU NEED TO MITIGATE THE HARM
TO THE EXTENT PRACTICABLE.

ALL RIGHT. NEXT SLIDE.

WE TALKED ABOUT THIS ALREADY.

THE PRIVACY RULE REQUIRES
THAT THERE BE TRAINING OF ALL

OF THE WORKFORCE THAT'S
NECESSARY AND APPROPRIATE

TO THEIR FUNCTIONS.

AND SO WHAT THAT MEANS IS THAT
YOU DON'T HAVE TO PROVIDE

THE SAME TRAINING TO EVERYBODY.

YOU JUST NEED TO PROVIDE
THE TRAINING THAT'S APPROPRIATE

TO THE JOB FUNCTIONS
OF THE PARTICULAR INDIVIDUALS.

SO, UM...IT MAY BE
IN SOME INSTANCES OVERKILL

TO HAVE THIS ORIENTATION
THAT SOME HOSPITALS DO.

I UNDERSTAND THEY DO IT
OUT OF EFFICIENCY.

WHERE THEY BRING IN ALL THE
NEW EMPLOYEES AND, AT THE SAME

TIME, PROVIDE THEM
WITH HIPAA TRAINING.

I DON'T KNOW IF THE
SECURITY GUARD NEEDS TO KNOW

ALL OF, YOU KNOW, THE RULES
AND REGS AND YOU COULD MAYBE

SAVE YOURSELF SOME TIME

BY HAVING SOME SORT
OF ABBREVIATED TRAINING

FOR THE GUY WHO'S JUST,
YOU KNOW, AT THE DOOR,

SO TO SPEAK.

YOU KNOW, ONE CAN'T IMAGINE
THAT HE'S GOING TO HAVE ACCESS

TO ELECTRONIC
HEALTH INFORMATION.

BUT THAT'S SOMETHING
TO KEEP IN MIND.

THE POINT HERE IS THAT
YOU DON'T HAVE TO PROVIDE

THE SAME
TRAINING TO EVERYONE.

AND THEN YOU NEED
TO DEVELOP AND APPLY A SYSTEM

OF SANCTIONS FOR EMPLOYEES
WHO VIOLATE YOUR POLICIES

AND PROCEDURES THAT ARE
REQUIRED BY THE PRIVACY RULE

AND THE SECURITY RULE.

UM...I THINK MOST COMPANIES
DO A GOOD JOB AT IMPOSING

SANCTIONS
AGAINST THEIR WORKFORCE.

WHAT WE FIND, HOWEVER, IS THAT
THEY DON'T HAVE IT WRITTEN DOWN,

THAT SANCTION POLICY,

OR THAT SANCTION MATRIX

IS NOWHERE TO BE FOUND
WHEN WE REQUEST ACCESS

TO THE SANCTION POLICY.

AND IT'S LIKE, UM...
"SANCTION POLICY?"

YEAH, YOU'RE SUPPOSED
TO HAVE A SANCTION POLICY,

A WRITTEN
SANCTION POLICY.

NOW, WE UNDERSTAND THAT YOU'VE
TAKEN THE APPROPRIATE ACTION,

AND PERHAPS YOU'VE ALREADY
DONE THAT, BUT THAT'S SUPPOSED

TO BE WRITTEN DOWN SO THAT
THE STANDARD IS APPLIED

CONSISTENTLY ACROSS THE BOARD.

SO THAT WHEN WE SAY--YOU KNOW,
A PERSON ALLEGES THAT THEY

WERE BEING RETALIATED AGAINST,
FOR EXAMPLE--AND WE'LL GET

TO THAT BECAUSE THAT'S IN THE
RULES AS WELL--WE CAN LOOK

AT YOUR SANCTION POLICY
TO SEE WHETHER OR NOT YOU ARE

CONSISTENTLY APPLYING
THE SAME SORT OF SANCTIONS

FOR THE SAME TYPE OF VIOLATION
ACROSS THE BOARD.

BECAUSE IF NOT, THEN THAT
MAY LEAD TO ONE TO CONCLUDE

THAT MAYBE THERE IS SOMETHING
TO THIS RETALIATION ALLEGATION.

IF THEY'VE BEING TREATED
DIFFERENTLY FOR THE SAME SORT

OF BREACH THAT SOMEBODY
ELSE MADE, AND YET, YOU KNOW,

THE SITUATIONS
ARE SIMILAR IN TERMS OF IT

WAS THE FIRST TIME, THERE WAS
SOMETHING RELATIVELY MINOR.

AND YET I WAS TERMINATED
AND SHE WASN'T.

>> [INDISTINCT]

>> NO, IT WOULD BE
A HIPAA ISSUE

IF THE EMPLOYEE ALLEGES
THAT THEY WERE ENGAGING

IN SOME SORT
OF PROTECTED ACTIVITY

UNDER THE PRIVACY RULE, AND THEN
BECAUSE THEY WERE DOING THAT,

THEY WERE TERMINATED.

FOR EXAMPLE, BEING
THAT YOU RAISED IT.

AND I'LL JUST GO
INTO IT BRIEFLY.

THE PERSON ALLEGES THAT THERE'S
A NURSE AT A NURSES' STATION,

AND THERE'S SOME
DOCTORS DOING ROUNDS,

AND THE DOCTORS ARE, YOU KNOW,
TALKING IN QUITE A LOUD VOICE,

AND THE NURSE COMES OVER AND
SAYS SOMETHING TO THE DOCTORS,

"COULD YOU LOWER
YOUR VOICES?

THERE'S VISITORS VISITING
THE PATIENTS HERE."

AND THE DOCTORS GET, YOU KNOW,
UPSET ABOUT IT, AND ONE DOCTOR,

WHO'S A SUPERVISOR, HAS THE
NURSE REPRIMANDED FOR SPEAKING

TO THE DOCTORS IN THAT MANNER.

SHE BELIEVES THAT SHE WAS
REPRIMANDED BECAUSE SHE TOLD

THEM SOMETHING THAT THEY
SHOULD HAVE BEEN AWARE OF

AND SHOULDN'T HAVE BEEN DOING.

AND SO BECAUSE OF THAT, SHE'S
REPRIMANDED AND SHE ALLEGES

THAT SHE WAS
RETALIATED AGAINST.

UM... WE GET THE COMPLAINT,
WE LOOK INTO THE COMPLAINT.

AND SO THE FIRST THING
WE ASK IS, YOU KNOW,

WAS SHE ENGAGED
IN A PROTECTED ACTIVITY?

WE GO THROUGH THIS ANALYSIS.

AND WE FIND OUT THAT SHE WAS.

AND THEN SHE FIND OUT--
WELL, SHE WAS, UM...

SHE SAID SHE'S
BEEN RETALIATED AGAINST

BECAUSE THE ACTION
WAS INAPPROPRIATE.

WE FIND OUT THAT SOMEBODY ELSE
HAD A SIMILAR SITUATION.

SIMILAR SITUATION.

SO WE LOOK AT BOTH
SITUATIONS TO SEE,

YOU KNOW, WAS THIS,
AS YOU ALLEGED,

A WORKPLACE
EMPLOYMENT ISSUE?

AND SHE WAS NOT--THERE WAS
NO ADVERSE ACTION TAKEN AGAINST

HER BECAUSE OF HER MAKING THEM
AWARE OF THE PRIVACY RULE,

OR WAS THIS ACTION TAKEN
AGAINST HER BECAUSE SHE SPOKE

TO THEM IN
AN INAPPROPRIATE MANNER?

AND SO WE ASK FOR, BEING THAT
WE HAVE THESE 2 SITUATIONS,

WE CONFRONT THEM WITH THEM--
WE WANT ACCESS TO THE OTHER

PERSON'S FILE AS WELL,
AND LOOK INTO THAT, AND SEE

WHAT WAS THE SANCTION
WITH RESPECT TO THAT INDIVIDUAL.

UM...ALL RIGHT.
NEXT SLIDE.

ALL RIGHT.

SO WE'RE GOING TO HAVE MISS
ROBINSON SPEAK TO YOU BRIEFLY

ABOUT THE SECURITY RULE.

>> THE SECURITY COVERS
ONLY PHI, WHICH IS

IN ELECTRONIC FORM.

THIS INCLUDES ELECTRONIC
PROTECTED HEALTH INFORMATION

WHICH IS CREATED, RECEIVED,
MAINTAINED, OR TRANSMITTED.

THE SECURITY RULE
WAS IMPLEMENTED

TO ADDRESS WHETHER
OR NOT THE ACTIONS

OF A COVERED ENTITY
ARE REASONABLE

FOR SAFEGUARDING

THE ELECTRONIC
HEALTH INFORMATION.

THE EXAMPLES THAT EPHI
MAY BE TRANSMITTED OVER

THE INTERNET,
EMAIL, STORED ON CDs,

ON DISKS,
PORTABLE HARD DRIVES,

PDAs, ALL OF THE TECHNOLOGY
THAT WE HAVE OUT NOW.

AND ALL OF THAT TECHNOLOGY
CAN HOLD PH--ELECTRONIC

PROTECTED
HEALTH INFORMATION.

AND A LOT OF TIMES LAPTOPS--

ALL OF THESE THINGS
ARE MOBILE

THAT WE MAY TAKE OUT
OF THE OFFICE AND USE.

THE COMPLIANCE DATES--

THE SECURITY RULE
WAS EFFECTIVE NO LATER

THAN APRIL 20
FOR ALL ENTITIES

EXCEPT SMALL
HEALTH PROVIDERS.

NO LATER THAN
APRIL 20, 2006

FOR THE SMALL
HEALTH PROVIDERS.

AT THE INCEPTION
OF THE SECURITY RULE,

CMS WAS
DELEGATED THE AUTHORITY

TO ADMINISTER AND ENFORCE
THE HIPAA SECURITY RULE.

AS OF JULY, 2009,

THE SECRETARY DELEGATED OCR
THE AUTHORITY

TO ADMINISTER AND ENFORCE
THE HIPAA SECURITY RULE.

SO NOW WE HAVE IT.

HA HA. NEXT SLIDE. HA HA.

COVERED ENTITIES MUST
ENSURE THE CONFIDENTIALITY,

INTEGRITY, AND AVAILABILITY
OF ALL EPHI,

WHICH THE COVERED ENTITY
CREATES, RECEIVES,

MAINTAINS, OR TRANSMITS.

WITH THIS,
ALSO THE IMPORTANCE

IS THAT PEOPLE OR PATIENTS
STILL HAVE ACCESS

TO THEIR ELECTRONIC

PROTECTED
HEALTH INFORMATION.

WE'RE FINDING THAT PEOPLE
ARE NO LONGER STORING

OR MAINTAINING HARD COPIES.

EVERYTHING IS
GOING ELECTRONIC.

EVERYTHING IS-- YOU KNOW,
A LOT OF PEOPLE HAVE--

A LOT OF ENTITIES HAVE

GOTTEN RID OF HARD COPIES
AND PAPERS, AND EVERYTHING

IS ELECTRONIC NOW. UM...

YOU CAN GO
TO THE NEXT SLIDE.

THE SECURITY RULE
ESTABLISHES

THE REQUIREMENTS
COVERED ENTITIES

AND BUSINESS
ASSOCIATES MUST MEET.

BECAUSE,
AS PREVIOUSLY STATED,

COVERED ENTITIES
ARE RESPONSIBLE

FOR THE ACTIONS OF THEIR
BUSINESS ASSOCIATES.

AND THIS ALL SHOULD
BE SPELLED OUT

IN THE BUSINESS
ASSOCIATE AGREEMENTS

THAT YOU HAVE WITH THEM
IN ORDER TO SHARE

INFORMATION WITH THEM.

UM...THE RULE ALSO INCLUDES
THE CONSIDERATION

FOR FLEXIBILITY,
FOR ENTITIES,

MEANING YOU HAVE
TO DEFINE YOUR INSTITUTION

AND WHAT MEETS YOUR
INSTITUTION VERSUS

A LARGE PROVIDER,
A SMALL PROVIDER.

YOU HAVE TO MAKE AN
ASSESSMENT OF YOUR ENTITY.

IT DEFINES
THE REQUIRED STANDARDS

AND THE IMPLEMENTATION
SPECIFICATIONS,

WHICH ARE BOTH
REQUIRED AND ADDRESSABLE.

AND I'LL DISCUSS THOSE,

I BELIEVE,
ON THE NEXT SLIDE.

THE SECURITY RULE ALSO
REQUIRES THE MAINTENANCE

OF SECURITY MEASURES
IMPLEMENTED TO SUPPORT THE

REASONABLE AND APPROPRIATE
PROTECTION OF ELECTRONIC

PROTECTED
HEALTH INFORMATION.

YOU CAN GO
TO THE NEXT SLIDE.

IF LIMITATION
SPECIFICATIONS,

THE SECURITY RULE
GIVES 2 TYPES.

THERE'S REQUIRED,
AND ADDRESSABLE.

REQUIRED MEANS
YOU ARE REQUIRED

TO IMPLEMENT
THAT SPECIFICATION.

ADDRESSABLE--
A COVERED ENTITY--

WE SAY THAT YOU NEED
TO ASSESS WHETHER

THE SPECIFICATION
IS REASONABLE

AND APPROPRIATE IN YOUR,
AGAIN, ENVIRONMENT.

IF YOU'RE NOT GOING
TO IMPLEMENT IT, THEN,

YOU KNOW,
YOU DO HAVE TO DOCUMENT

THAT YOU'RE NOT IMPLEMENTING
A SPECIFICATION.

OR IF YOU'RE GOING
TO USE SOMETHING

THAT'S EQUIVALENT TO
THAT, WHEREAS TO ONE ENTITY

MAY USE ANOTHER METHOD--

WHEREAS YOU SAY, "NO,
WE'RE NOT GOING TO USE THAT,

"BUT WE'RE GOING TO
USE SOMETHING ELSE.

SOMETHING EQUIVALENT
TO THAT."

THE SECURITY RULE IS REALLY
BASED OFF OF YOUR DESIGN

BECAUSE EVERY ENTITY
IS NOT RAN THE SAME WAY.

EVERY ENTITY DOES NOT HAVE
THE SAME TECHNOLOGY.

SOME HAVE MORE
ADVANCED TECHNOLOGY,

SOME MAY JUST KNOW
HOW TO USE THE INTERNET,

OR JUST KNOW HOW
TO SEND AN EMAIL,

WHERE OTHERS
ARE DOING THINGS THAT ARE

FAR MORE ADVANCED.

YOU CAN GO
TO THE NEXT SLIDE.

THE SECURITY RULE DEALS WITH
ADMINISTRATIVE SAFEGUARDS,

TECHNICAL SAFEGUARDS...

AND THE RULE DOES ADDRESS--

AND PHYSICAL SAFEGUARDS.

THE RULE ADDRESSES
ALL OF THESE 3 TYPES

THAT AN ENTITY MUST
REVIEW OR MUST IMPLEMENT,

WHICH ARE ADDRESSABLE.

SOME ARE ADDRESSABLE
UNDER ALL 3.

SOME ARE REQUIRED
UNDER ALL 3.

UNDER ADMINISTRATIVE
SAFEGUARDS--

THE ADMINISTRATIVE--
HERE'S WHERE YOU ADDRESS

THE ADMINISTRATIVE ACTIONS,

AND THE POLICIES
AND PROCEDURES

WHERE YOU'RE
IMPLEMENTING TO MAINTAIN

THE SECURITY OF ELECTRONIC

PROTECTED
HEALTH INFORMATION.

AND THE CONDUCT OF THE
COVERED ENTITY'S WORKFORCE

IN RELATION
TO THE PROTECTION

OF THAT INFORMATION.

MAKING SURE THAT YOU TRAIN
YOUR STAFF TO LET THEM KNOW

THAT, YOU KNOW,
THIS INFORMATION HAS TO BE

SAFEGUARDED,
WHETHER IT'S SOMEONE

WORKING ON A COMPUTER,

AND YOU HAVE PATIENTS THAT
COME IN THE FACILITY--

HOW IS YOUR

COMPUTER SCREEN SET UP?

IS IT SET UP THAT
INDIVIDUALS CAN JUST WALK IN

AND ACTUALLY SEE
PATIENTS' NAMES

AND DIAGNOSES
ON THE COMPUTERS?

OR IS THERE A WALL,

OR IS THERE A GLASS
THERE PROTECTING

THE COMPUTER SO THAT IT'S
ONLY VISIBLE TO STAFF?

YOU CAN GO
TO THE NEXT ONE.

PHYSICAL SAFEGUARDS--

PHYSICAL MEASURES, POLICIES

AND PROCEDURES TO PROTECT
COVERED ENTITIES ELECTRONIC

INFORMATION SYSTEMS RELATED
TO BUILDINGS, EQUIPMENT,

FOR NATURAL AND
ENVIRONMENTAL HAZARDS,

AND UNAUTHORIZED
INTRUSIONS,

MEANING IF PEOPLE
CAN LITERALLY HACK

INTO YOUR SYSTEMS.

UM...NATURAL DISASTERS--

IF YOU HAVE
ANY BACK-UP MEASURES.

IF EVERYTHING
WERE TO GO DOWN,

ARE YOU GOING TO LOSE
ALL YOUR DATA?

DO YOU STILL HAVE IT?

CAN YOU RETAIN YOUR DATA?

DO YOU HAVE, UM...SYSTEMS
IN PLACE IF IT'S AN OUTAGE?

OR, YOU KNOW, IS ALL THE
DATA GOING TO BE WIPED OUT

OF THE SYSTEM?
CAN YOU RETRIEVE IT?

DO YOU HAVE A METHOD
OF RETRIEVING IT?

AND SOME OF
THESE ARE REQUIRED

AND SOME ARE ADDRESSABLE.

YOU CAN GO TO THE NEXT ONE.

A COVERED ENTITY
MUST IMPLEMENT

TECHNICAL SAFEGUARDS.

IT MEANS THE TECHNOLOGY,
AND THE POLICY,

AND PROCEDURES FOR ITS USE

THAT PROTECT ELECTRONIC
PROTECTED HEALTH

INFORMATION AND
CONTROL ACCESS TO IT.

SOME OF THESE MAY BE
REQUIRED OR ADDRESSABLE.

>> OK, THESE SLIDES HERE
ARE A LITTLE BIT DIFFERENT

FROM THE SLIDES THAT WERE

SUBMITTED TO GIVE YOU

AN EXAMPLE OF WHAT WOULD BE
REQUIRED AND WHAT WOULD BE

ADDRESSABLE UNDER
ADMINISTRATIVE SAFEGUARDS.

SOME EXAMPLES--SOME PEOPLE
SAY, "WELL, WHAT DO YOU MEAN

BY REQUIRED? WHAT DO YOU
MEAN BY ADDRESSABLE?"

WHAT'S REQUIRED?
WHAT'S ADDRESSABLE?

THAT'S ONE GOOD THING
ABOUT THE SECURITY RULE,

IF YOU LOOK AT THE RULE AND
GO THROUGH THE RULE,

THERE'S AN "R"
FOR REQUIRED

AND AN "A" FOR
WHAT'S ADDRESSABLE.

SO YOU KNOW, WELL,
OUR ENTITY NEEDS TO,

AND IT'S REQUIRED
TO HAVE THESE IN PLACE,

BUT THIS MAY BE ADDRESSABLE,
WHERE IT'S NOT REQUIRED,

BUT WE MAY NEED
TO IMPLEMENT IT,

BUT WE NEED
TO ACTUALLY ADDRESS THIS.

AND WHEN WE'RE
DOING INVESTIGATIONS

FOR SECURITY RULE,
WE'LL ASK YOU,

"DID YOU ADDRESS IT?"

AND IF YOU ADDRESSED IT,

YOU REALLY
NEED TO DOCUMENT IT.

EVERYTHING IS
ABOUT DOCUMENTATION.

IF YOU'RE ADDRESSING,
YOU MAY SAY,

"WELL,
WE DID ADDRESS THIS.

"HOWEVER, THIS DOESN'T
SUIT OUR ENTITY,

"SO WE DIDN'T NEED
TO IMPLEMENT THIS.

BUT WE DOCUMENTED IT."

AND ANOTHER THING
THAT WE ALSO LOOK AT

IS DO YOU GO BACK
AND REVIEW YOUR POLICY?

DO YOU GO EVERY 6 MONTHS
AND REVIEW THEM?

DO YOU LOOK
AT THEM EVERY YEAR?

BUT AT SOME POINT WE WANT
TO KNOW, YOU KNOW,

IF YOU CHANGED,
DID YOU GO BACK

AND REVIEW YOUR POLICIES?

FOR ADMINISTRATIVE
SAFEGUARDS,

WHAT WOULD BE REQUIRED
IS RISK ANALYSIS.

RISK ANALYSIS
YOU WOULD ADDRESS,

ARE VULNERABILITIES
IDENTIFIED?

ARE RISKS CALCULATED
TO DETERMINE

THE IMPACT TO EPHI?

RISK MANAGEMENT IS
ALSO A REQUIREMENT.

UNDER RISK MANAGEMENT, YOU
WANT TO CHECK, ARE RISKS

AND VULNERABILITIES
REDUCED TO A REASONABLE

AND APPROPRIATE LEVEL?

DID YOU ASSESS IT TO
DETERMINE THAT--

IS THIS A SMALL RISK,
OR IS THIS A LARGE RISK?

IF YOU CAN DETERMINE THAT
SOMETHING IS A LARGE RISK,

WHAT DID YOU DO TO IMPLEMENT
SAFEGUARDS TO PROTECT IT?

ALSO, WHAT'S REQUIRED IN
ADMINISTRATIVE SAFEGUARDS

IS SANCTION POLICY,
SUCH AS IT IS IN PRIVACY.

ARE METHODS UTILIZED TO
INFORM WORKFORCE MEMBERS

ABOUT SANCTION POLICIES
FOR NON-COMPLIANCE?

DID YOU TELL YOUR STAFF,
IF YOU'RE IMPERMISSIBLY

ACCESSING SOMEONE'S PHI,

YOU KNOW, WE CAN TRACK THIS,

AND THERE ARE SANCTIONS
THAT ARE IMPOSED.

WE GET A LOT OF COMPLAINTS
ON THE SECURITY SIDE WHERE

SOMEONE WILL SAY, "WELL,
YOU KNOW, MY SISTER-IN-LAW

"WORKS IN THIS HOSPITAL,

"AND I CAME IN
THERE--WE DON'T GET ALONG,

"AND SHE ACCESSED

"MY PROTECTED
HEALTH INFORMATION.

IF SHE HAD NO
REASON TO ACCESS IT,

THAT'S
AN IMPERMISSIBLE ACCESS.

AND STAFF NEEDS
TO REALLY BE AWARE

THAT IF YOU'RE
ACCESSING INFORMATION--

ELECTRONIC PROTECTED
HEALTH INFORMATION--

FOR SOMETHING OUTSIDE OF
WORK-RELATED PURPOSES,

THERE ARE SANCTIONS THAT
ARE GOING TO BE IMPOSED.

AND WE DO LOOK AT THEM.

WE WILL ASK FOR, AS ERIC
EXPLAINED, WE WILL ASK FOR,

"WELL, LET'S SEE
YOUR SANCTION POLICY?"

DID YOU APPROPRIATELY
SANCTION THIS EMPLOYEE?"

SO WE REALLY DO BELIEVE

THAT STAFF NEEDS
TO UNDERSTAND THAT.

NOW UNDER
ADMINISTRATIVE SAFEGUARDS,

WHAT IS ADDRESSABLE?

WORKFORCE
CLEARANCE PROCEDURE.

NO ONE KNOWS THEIR WORKPLACE
LIKE YOU, SO, YOU KNOW,

THERE YOU WOULD ADDRESS, ARE
WORKFORCE MEMBERS ALLOWED

TO ACCESS MORE
THAN MINIMUM NECESSARY

TO PERFORM
THEIR JOB FUNCTION?

HMM. DOES A STAFF MEMBER
HAVE ACCESS

THAT THEY REALLY
DON'T NEED?

THAT'S SOMETHING THAT
AS SECURITY OFFICERS,

COMPLIANCE OFFICERS, YOU
NEED TO DETERMINE WHAT STAFF

NEEDS TO DO THEIR JOB.

ARE YOU GIVING THEM MORE
THAN WHAT'S NECESSARY?

DO THEY REALLY NEED TO KNOW
ALL OF THIS INFORMATION?

OR THEY HAVE THE INFORMATION

THAT THEY NEED
TO GET THE JOB DONE.

ANOTHER ADDRESSABLE UNDER
ADMINISTRATIVE SAFEGUARDS

IS LOG-IN MONITORING,

EMPHASIZING
OUR FAILED SYSTEMS

AND APPLICATION LOG-IN
ATTEMPTS RECORDED

AND REVIEWED.

EVERY TIME SOMEONE
TRIES TO ATTEMPT

TO LOG-IN, IS THAT
RECORDED SOMEWHERE?

ARE YOU ABLE TO DETERMINE
THAT MAYBE SOMEONE

WAS TRYING TO ACCESS OR USE
SOMEONE ELSE'S PASSWORD

AND CODE TO GET IN?

ARE YOU ABLE TO KEEP
TRACK OF THESE THINGS?

BECAUSE, BELIEVE IT OR NOT,
WE GET COMPLAINTS FROM STAFF

MEMBERS THAT WILL TELL US

LITTLE SMALL THINGS
LIKE THIS,

ESPECIALLY
DISGRUNTLED EMPLOYEES.

AND WE DO HAVE
TO LOOK AT THAT.

THEY'LL SAY, "WELL, THERE'S
NO PASSWORD PROTECTION.

"YOU CAN SIT THERE
AND TRY AND ATTEMPT

"TO LOG-IN 15-20 TIMES

AND TRY TO GUESS WHAT
A PASSWORD IS."

WELL, IS THAT REASONABLE?

SHOULD THEY BE LOCKED
OUT AT THAT POINT?

SHOULD THEY HAVE TO GO TO
I.T. AND HAVE THEM LOOK AT,

YOU KNOW, CHANGING
THEIR PASSWORD?

ANOTHER THING IS
PASSWORD MANAGEMENT.

THAT'S ANOTHER THING.

YOU WILL LOOK AT,
ARE WORKFORCE MEMBERS

REQUIRED TO CHANGE PASSWORDS
ON A PERIODIC BASIS?

I HAD A CALL
NOT TOO LONG AGO.

THEY ASKED US, "HOW MANY
TIMES SHOULD WE HAVE THEM

CHANGE THEIR PASSWORD?"

SHOULD IT BE EVERY 6 MONTHS,
ONCE A YEAR,

ONCE EVERY OTHER MONTH?

WE SAY THAT'S
ADDRESSABLE TO THE ENTITY.

YOU MAKE THAT DETERMINATION
AS TO WHETHER THEY NEED

TO CHANGE IT EVERY 2 MONTHS,

EVERY 3 MONTHS.

IF YOU FEEL AS THOUGH YOU'RE
COMPANY MAY BE VULNERABLE,

THEIR ELECTRONIC PROTECTED
HEALTH INFORMATION,

YOU MAY WANT TO HAVE TO
CHANGE IT EVERY 6 WEEKS.

OR YOU MAY SAY, "WELL,
WE DON'T BELIEVE THAT,

SO WE HAVE THEM
CHANGE IT EVERY 6 MONTHS."

ALSO,
WORKFORCE MEMBERS TRAINED

ON PASSWORD COMPLEXITY
AND LENGTH.

IS THE PASSWORDS
JUST 3 WORDS THAT ANYBODY

CAN GUESS, OR ARE YOU
HAVING THEM USE CAPITALS,

CAPITAL LETTERS,
SPECIAL CHARACTERS?

I KNOW OURS IS CAPITALS,
SPECIAL CHARACTERS,

EXCLAMATION POINTS, LETTERS,

NUMBERS, ALL MIXED
IN ONE PASSWORD.

AND THE STRENGTH
OF THAT DOES DETERMINE

THE COMPLEXITY
OF WHETHER OR NOT PEOPLE

MAY BE ABLE TO USE
SOMEONE ELSE'S PASSWORD

AND ACCESS IT.

YOU CAN GO TO
THE NEXT SLIDE.

I DON'T KNOW IF
IT'S THE SAME SLIDE.

NO. BUT I'M NOT FINISHED.

YOU CAN STAY THERE.
I'LL SAY IT.

>> OK.

>> THEY DIDN'T SEND
THE CORRECT SLIDES

TOWARDS THE END. ALSO,
PHYSICAL SAFEGUARDS.

PHYSICAL SAFEGUARDS ARE
THE PHYSICAL MEASURES

IMPLEMENTED TO PROTECT
COVERED ENTITIES,

EPHI SYSTEMS
AND EQUIPMENT.

SOME REQUIRED UNDER
PHYSICAL SAFEGUARDS

WOULD BE FACILITY
ACCESS CONTROLS.

THESE ARE THINGS THAT
YOU WANT TO LOOK AT

THAT, ARE FACILITY
LOCATIONS WHERE EPHI'S

ACCESS IS
STORED IDENTIFIED?

DO YOU KNOW EVERY PLACE
IN YOUR FACILITY

WHERE YOU HAVE
COMPUTERS AT?

DO YOU KNOW
WHERE THE COMPUTERS

ARE LOCATED AT?
WE GET A LOT OF THEFT

OF LAPTOPS FROM
OUT OF FACILITIES.

WHEN WE GO BACK
AND ASK THEM,

"DID YOU KNOW A LAPTOP
WAS THERE?"

SOME OF THEM SAY, "NO,
WE DIDN'T KNOW LAPTOPS

WAS IN THAT AREA."

SO THAT'S NOT
A GOOD THING.

ARE AREAS OF THE
FACILITY PUBLICLY

ACCESSIBLE AND HOW
ARE THEY MONITORED?

DO YOU HAVE A ROOM WITH
LAPTOPS IN IT THAT HAVE

ELECTRONIC PROTECTED
HEALTH INFORMATION

BUT THE PUBLIC CAN
ACCESS IT?

CAN THE PUBLIC COME IN?

CAN SOMEBODY
JUST SIT DOWN, OPEN UP

THE COMPUTER AND JUST
GET ON IN IT AND

THERE'S ELECTRONIC
PROTECTED HEALTH

INFORMATION

STORED ON A LAPTOP?

THOSE ARE THINGS THAT
FACILITIES, COMPLIANCE

OFFICERS
NEED TO ADDRESS.

WHERE IS ELECTRONIC
PROTECTED

HEALTH
INFORMATION STORED

AND WHERE IS ITS
LOCATION PHYSICALLY?

WHERE IS IT AT?

PDA_s AND STUFF--THAT'S
ANOTHER THING TO REMIND

STAFF. DON'T LEAVE
THOSE LAYING AROUND.

YOU KNOW, SOMETIMES
PEOPLE, YOU PUT

YOUR PHONE DOWN,
OR, YOU KNOW,

AND ALSO LIKE, UM...

PORTABLE USB_s AND
THINGS OF THAT NATURE.

YOU KNOW, BE VERY
MINDFUL OF WHERE

YOU'RE PUTTING
THINGS DOWN.

ARE YOU DROPPING
THEM ON DESKS?

DO THE PUBLIC HAVE
ACCESS TO THAT?

THOSE ARE THINGS THAT
YOU WANT TO MAKE STAFF--

YOU KNOW,
KEEP REMINDING THEM OF.

ALSO, WHICH IS
REQUIRED IS DISPOSAL.

ARE MEDIA HARDWARE
DESTRUCTION PROCEDURES,

ASSIGNED, DOCUMENTED,
AND VERIFIED?

THAT'S ANOTHER THING.

WE'VE GOTTEN
CALLS ON THAT.

HOW DO YOU
DESTROY ELECTRONIC

PROTECTED
HEALTH INFORMATION?

ARE YOU DESTROYING DISKS

THAT YOU MAY
NO LONGER NEED?

ARE YOU WIPING OUT USBs

THAT YOU NO LONGER
ARE USING

OR ARE YOU JUST
THROWING THEM AWAY?

ARE YOU THROWING THEM IN
THE GARBAGE, YOU KNOW,

ARE YOU THROWING
DISKS IN THE GARBAGE?

ALL OF THOSE THINGS
NEED TO BE LIKE

HARD DRIVES--SCRUBBED
AND INFORMATION

DELETED FROM THERE.

AND SOMETIMES, ACTUALLY,

DELETING
DOESN'T REALLY DELETE.

THAT'S ANOTHER THING.

WE'VE HAD ENTITIES
TO CALL AND SAY,

"WE'RE GOING TO GIVE
AWAY OUR COMPUTERS.

WE GOT BRAND-NEW
COMPUTERS."

YOU KNOW, "WHAT ARE WE GOING
TO DO WITH THE HARD DRIVES?"

THERE ARE PROGRAMS OUT THERE
THAT WILL ACTUALLY DELETE.

PEOPLE THINK THAT YOU'RE
DELETING, YOU'RE REALLY

DELETING INFORMATION,
BUT YOU'RE NOT ACTUALLY

DELETING IT. THERE ARE
PROGRAMS OUT THERE

THAT WILL DELETE DELETE
THE INFORMATION.

SO WE TELL PEOPLE BE MINDFUL
THAT NO ONE CAN RETRIEVE IT.

SOME PEOPLE WANTED TO GIVE
AWAY COMPUTERS TO THE BOYS

AND GIRLS CLUB. UM...

ADDRESSABLE WOULD BE
DATA BACKUP, STORAGE.

ARE PROCEDURES IN
PLACE TO BACK UP DATA?

THINGS LIKE THAT
ARE ADDRESSABLE.

UNDER TECHNICAL SAFEGUARDS
YOU HAVE REQUIRED,

WHICH ARE LIKE I DISCUSSED,

USER--UNIQUE USER
IDENTIFICATIONS.

THOSE ARE REQUIRED.

AUDIT CONTROL
STANDARDS ARE REQUIRED.

ARE REVIEWS OF SYSTEM AUTO
LOGS PERFORMED PERIODICALLY?

HOW MANY TIMES ARE YOU--
ARE YOU ADDRESSING THAT,

ARE YOU
LOOKING AT THAT?

ADDRESSABLE WOULD
BE SOMETHING LIKE

AUTOMATIC LOG-OFF.
DOES THE SYSTEM

AUTOMATICALLY
LOG ITSELF OFF?

DOES IT AUTOMATICALLY TURN
ITSELF OFF

WHEN YOU WALK AWAY
FROM THE COMPUTER?

THOSE THINGS LIKE THAT
YOU WANT TO ADDRESS.

I'M GOING TO GIVE IT
TO ERIC TO DO THE BREACH.

HA HA. SO HE CAN GO
OVER THE BREACH.

>> YEAH, YEAH, YEAH.

OK, WHAT I'M GOING TO DO

IS I'M GOING TO GO THROUGH

JUST MAYBE 3 OR 4 SLIDES OF
THE BREACH NOTIFICATION RULE

SO THAT WE CAN HAVE
AT LEAST 5 OR 6 MINUTES

FOR SOME QUESTIONS.

THE BREACH NOTIFICATION RULE
IS SOMETHING THAT WENT

INTO EFFECT JUST RECENTLY,
LAST SEPTEMBER OF 2009,

AND IT APPLIES TO ALL
TYPES OF BREACHES--

BREACHES INVOLVING
THE PRIVACY RULE,

AS WELL AS THE SECURITY RULE.

AND WHAT THE BREACH
NOTIFICATION RULE STATES

BASICALLY IS THAT A COVERED
ENTITY HAS TO PROVIDE NOTICE

TO OCR IF A BREACH INVOLVES
1, IF IT'S LESS THAN 500

INDIVIDUALS, THEN YOU MUST
PROVIDE NOTICE TO OCR.

IF THE BREACH INVOLVES MORE
THAN 500 INDIVIDUALS,

YOU MUST
PROVIDE NOTICE TO OCR.

HOWEVER, DISTINCTION IS
THAT FOR THOSE BREACHES THAT

INVOLVE MORE THAN 500
INDIVIDUALS, YOU ALSO MUST

GIVE NOTICE TO THE MEDIA ABOUT
THE BREACH, SO HAVE TO PUT OUT

SOME SORT OF PRESS STATEMENT
INDICATING THAT THERE'S BEEN

A BREACH WITH RESPECT TO THE
PRIVACY OR THE SECURITY RULE

AND THAT ALL INDIVIDUALS WHO
MAY BE IMPACTED CAN CONTACT

THE COVERED ENTITY TO SEE HOW
IT'S GOING TO BE ADDRESSED.

WHAT'S CRITICAL ABOUT THE
NOTICE IS THAT YOU HAVE

AN OBLIGATION TO GIVE NOTICE
WITHIN 60 DAYS FROM THE DATE

THAT YOU DISCOVERED THE BREACH
WITHOUT AN UNREASONABLE DELAY.

SO WHAT HAPPENS OFTENTIMES IS
THAT YOU MAY NOT BE AWARE THAT

A BREACH HAS OCCURRED, AND
SO YOUR 60 DAYS DOES NOT

START RUNNING.

HOWEVER, THERE'S
A REASONABLE PERSON STANDARD.

AND LAWYERS LIKE LANGUAGE
LIKE "REASONABLE,"

AND SO THAT IF
YOU SHOULD HAVE KNOWN

WITHIN A CERTAIN PERIOD
OF TIME,

THEN THE CLOCK STARTS
TICKING FROM THAT PERIOD.

YOU CAN GO TO THE NEXT SLIDE.

A BREACH IS DEFINED
IN THE RULE FOR YOU

AS AN IMPERMISSIBLE ACQUISITION,
ACCESS, USE, OR DISCLOSURE

OF PHI IN A MANNER THAT'S NOT
PERMITTED UNDER EITHER

THE PRIVACY RULE OR THE SECURITY
RULE, AND IT COMPROMISES

THE SECURITY OR THE PRIVACY
OF SOMEONE'S PROTECTED

HEALTH INFORMATION.

THAT'S THE TECHNICAL
DEFINITION OF A BREACH,

AND IT'S PRETTY MUCH THE SAME
WAY YOU DEFINE BREACH

RIGHT NOW
FOR PURPOSES OF PRIVACY.

UM...WE TAKE THAT DEFINITION
AND THEN WE PICK IT APART.

WHAT DO WE MEAN WHEN WE SAY
TO COMPROMISE A SECURITY

OR A PRIVACY?

WHAT WE MEAN BY IS THAT
IS THE BREACH MUST POSE

A SIGNIFICANT RISK,
A FINANCIAL, REPUTATIONAL,

OR OTHER HARM TO
THE INDIVIDUALS

WHOSE PROTECTED
HEALTH INFORMATION

WAS IMPERMISSIBLY USED,
ACCESSED, OR DISCLOSED.

YOU CAN GO TO THE NEXT SLIDE.

UM, THIS IS WHERE
THE COVERED ENTITY HAS

ANOTHER RESPONSIBILITY.

NOT ONLY DO YOU HAVE
TO PROVIDE NOTICE UNDER

THE BREACH NOTIFICATION RULE
WITHIN REASONABLE TIME,

OR NO LESS THAN 60 DAYS AFTER
YOU DISCOVERED THE BREACH,

BUT YOU ALSO MUST ENGAGE IN
WHAT WE CALL A RISK ASSESSMENT

ONCE YOU LEARN OF THE BREACH
IN ORDER TO DETERMINE WHETHER

OR NOT THE PHI THAT WAS
IMPERMISSIBLY USED, ACCESSED,

OR DISCLOSED WAS WHAT
WE CALL UNSECURED PHI.

AND BEING UNSECURED PHI,
WHETHER OR NOT THAT POSED

A SIGNIFICANT RISK OF
REPUTATIONAL, OR FINANCIAL,

OR OTHER TYPE OF HARM
TO THE INDIVIDUAL.

SO YOU HAVE AN ASSESSMENT
OBLIGATION, A PROACTIVE

OBLIGATION TO DO SOMETHING
ONCE YOU BECOME AWARE

OF A BREACH OF UNSECURED PHI.

>> WHAT WE'RE GOING
TO HAVE HERE IS A COUPLE

OF EXAMPLES OF WHAT
WE MEAN WHEN WE TALK

ABOUT A RISK OF HARM.

HERE YOU CAN SEE IF THE CE

MISTAKENLY DISCLOSES THE PHI
TO THE WRONG PHARMACY, BECAUSE
THE PHARMACY IS ALSO A CE
AND OBLIGATED TO COMPLY WITH
THE SECURITY AND THE PRIVACY
RULES, THIS MAY NOT POSE
A SIGNIFICANT RISK OF HARM
TO THE INDIVIDUAL.

WHAT THAT MEANS IS YOU HAVE
2 COVERED ENTITIES--

ONE DISCLOSES INFORMATION
TO THE OTHER COVERED ENTITY.

WHEN YOU DO YOUR RISK
ASSESSMENT, ONE CAN REASONABLY

CONCLUDE THAT THERE'S PROBABLY
NOT A SIGNIFICANT RISK OF HARM

OF EITHER FINANCIAL,
REPUTATIONAL, OR OTHER HARM,

TO THE PERSONS WHOSE PHI
WAS IMPERMISSIBLY USED,

ACCESSED, OR DISCLOSED.

WE CAN REASONABLY CONCLUDE
THAT BECAUSE IF IT'S NOT SOME

SORT OF, YOU KNOW, DIVE,
HOLE-IN-THE-WALL TYPE

OF PHARMACY THAT ONE
SHOULD BE SUSPICIOUS ABOUT

FROM THE OUTSET, THEN
THE PHI IS PRETTY MUCH SECURE.

UM, IF THE CE LOSES AN ENCRYPTED
LAPTOP WHERE THE INFORMATION

WAS NOT SECURED, OR WHERE
THE INFORMATION WAS SECURED

BECAUSE--WELL, IF IT'S NOT
SECURED, IF IT'S NOT ENCRYPTED.

AND THEN THEY DISCOVER
THAT THE NEXT DAY

THAT, YOU KNOW, THE INFORMATION
WAS NOT OPENED.

HOWEVER, THEN THAT MAY NOT POSE
A SIGNIFICANT RISK OF HARM.

THAT ONE'S A LITTLE TROUBLING,
YOU KNOW, FOR ME PERSONALLY,

BECAUSE, YOU KNOW, YOU THEN HAVE
TO ENGAGE OR HIRE SOME SORT

OF, YOU KNOW, FORENSIC SCIENTIST
OR COMPUTER EXPERT TO FIND OUT

WHETHER OR NOT THE INFORMATION
WAS ACTUALLY ACCESSED.

AND I'M NOT SURE,
YOU KNOW,

BUT I'M NOT A COMPUTER
TECH PERSON EITHER,

WHETHER OR NOT YOU CAN BE
CERTAIN, YOU KNOW,

THAT SOMEONE WHO'S
JUST AS GOOD

AS THE FORENSIC EXPERT
CANNOT LEAVE TRACES

THAT THEY ACCESSED THE PHI.

SO THAT TROUBLES ME A LITTLE,

BUT THAT'S THE WAY
THE RULE WORKS OUT

THAT IF YOU HIRE
A FORENSIC ANALYST AND THEY

REVEAL THAT THE INFORMATION
WAS NOT ACCESSED, EVEN THOUGH

THE LAPTOP WAS LEFT SOMEPLACE,

SAY, MIDTOWN
AT THE PORT AUTHORITY,

THEN THE RULE DETERMINES
THAT IT DOESN'T

IMPOSE A SIGNIFICANT RISK
OF INDIVIDUAL HARM.

EXCEPTIONS TO
THE DEFINITION OF A BREACH

IS THAT IF A PERSON
IS ACTING WITHIN AUTHORITY,

OR WITHIN THE SCOPE
OF THEIR EMPLOYMENT,

AND THEY DISCLOSE OR USE
THE INFORMATION IN GOOD FAITH,

AND WE CAN REASONABLY
BE ASSURED

THAT THERE WAS NO FURTHER
IMPERMISSIBLE USE

OF DISCLOSURE OF THE PHI,
THEN WE SAY THAT, YOU KNOW,

THERE HASN'T BEEN A BREACH.

UM...TECHNICALLY,
THERE'S BEEN A BREACH,

BUT THE RULE WOULD NOT
CLASSIFY THAT AS A BREACH.

AND I'LL JUST GIVE YOU
A QUICK EXAMPLE OF THAT.

THAT'S THE SITUATION WHERE
A NURSE SPEAKS TO A DOCTOR

ABOUT A PATIENT WHO

SHE BELIEVED WAS A PATIENT

OF THE DOCTOR. AND THEN AFTER,
YOU KNOW, A FEW MINUTES

THE DOCTOR SAYS TO THE NURSE,
"OH, THAT'S NOT MY PATIENT."

IN THAT SITUATION,

SHE WAS ACTING WITHIN
THE SCOPE OF HER EMPLOYMENT.

SHE DID IT IN GOOD FAITH
THINKING THAT SHE WAS UPDATING

THE DOCTOR ABOUT HIS PATIENT
BECAUSE HE JUST CAME OFF

OF ROUNDS, AND THAT THERE
IS NO RISK OF ANY FURTHER

IMPERMISSIBLE USE OR
DISCLOSURE OF THE PSI.

SO THAT WOULDN'T BE
CONSIDERED A BREACH.

UM...LET'S GO
ONTO THE NEXT SLIDE.

ANOTHER SITUATION THAT
YOU HAVE OF AN UNINTENTIONAL

ACQUISITION IS IF YOU HAVE
A BUILDING EMPLOYEE WHO RECEIVES

AND OPENS EMAIL ABOUT
A PATIENT THAT WAS MISTAKENLY

SENT TO HER
AT THE SAME FACILITY.

AND SHE ALERTS THE NURSE,

AND THE NURSE DELETES
THE EMAIL.

AGAIN, THIS IS AN
UNINTENTIONAL ACCESS OF PHI.

IT'S PRETTY CLEAR HERE.

AND IT WOULDN'T CONSTITUTE
A BREACH AS LONG AS THE NURSE

WHO OPENED UP AND READ THE EMAIL
OR THE BILLING EMPLOYEE

DIDN'T FURTHER DISCLOSE IT.

GO ONTO THE NEXT SLIDE.

UM...WHAT I'LL DO
IS I'LL STOP HERE

BECAUSE THESE ARE ALL
EXAMPLES, AND YOU HAVE THEM

IN YOUR PACKAGE, AND I
GOT MAYBE 1 OR 2 MINUTES,

OR 3 MINUTES FOR SOME
QUESTIONS IF ANYBODY

HAS ANY QUESTIONS.
OK, YES?

>> I'M GOING
TO USE THE MIC.

THAT WAY WE'LL HAVE
THIS RECORDED

AND EVERYONE CAN HEAR.

>> ONCE A WEEK
OR SO MY COMPANY--

MY COLLEAGUES AND I GO
OUT TO THE WEBSITE,

TO LOOK AT THE BREACHES
THAT HAVE OCCURRED

AFFECTING MORE
THAN 500 PEOPLE.

BUT WE HAVE NOT SEEN YET ANY
INFORMATION ABOUT HOW OCR OR

HHS HAS HANDLED
THOSE SITUATIONS.

SO THAT'S WHAT
WE'RE LOOKING FOR.

WE'RE KIND OF LOOKING
FOR A BENCHMARK

AS TO WHAT WE CAN
EXPECT IF THE BREACH

IS AT, YOU KNOW, "A"
SEVERITY THIS IS HOW

THE AGENCY HANDLED IT,
IT WAS AT "B" SEVERITY.

THIS IS HOW THE
AGENCY HANDLED IT,

SO THAT WE MAY KNOW
KIND OF WHAT TO EXPECT

AS WE'RE BRIEFING
OUR INTERNAL LEADERSHIP

WHEN WE HAVE AN ISSUE.

>> OK. SOME QUICK
COMMENTS ABOUT THAT.

AS I SAID, THE RULE IS
PRETTY NEW IN TERMS OF RULES

IN GOVERNMENT. IT'S ONLY BEEN
IN EFFECT ABOUT MAYBE 7,

8, 9 MONTHS ACTUALLY.

WHAT HAPPENS IS ONCE WE LEARN
OF A BREACH AND IT'S REPORTED

AFFECTING 500 OR MORE PEOPLE,

WE THEN USUALLY WILL
INITIATE AN INVESTIGATION.

BECAUSE THE RULE IS STILL

SO NEW, THERE ARE A NUMBER
OF BREACHES INVOLVING 500 OR
MORE PEOPLE AND THOSE CASES

ARE IN
THE INVESTIGATIVE STAGE.

AND SO WE HAVE TO GO
THROUGH A PROCESS

AND ANALYSIS AS TO WHY
THE BREACH OCCURRED,

IF IT INVOLVED ELECTRONIC,
YOU KNOW, PROTECTED

HEALTH INFORMATION, YOU KNOW,

WHAT SYSTEM
THEY HAVE IN PLACE--

ALL THE STUFF THAT KELLI
TALKED ABOUT WITH RESPECT

TO THE SECURITY RULE.

AND THEN WE ALSO
HAVE TO LOOK AT IT

FROM A PRIVACY
RULE STANDPOINT.

SO THOSE ARE,
YOU KNOW, VERY EXHAUSTIVE,

IN-DEPTH INVESTIGATIONS THAT
YOU'RE NOT GOING TO SEE

ANYTHING, YOU KNOW, ON THE OCR
WEBSITE AT THIS POINT

UNTIL THOSE INVESTIGATIONS
ARE COMPLETE.

>> BUT CAN WE EXPECT TO SEE
SOMETHING IN TERMS OF OCRs

DECISION MAKING
IN THOSE INSTANCES?

>> YEAH, YEAH, THERE'LL
BE INFORMATION.

WE HAVE REPORTING REQUIREMENTS
TO CONGRESS WITH RESPECT

TO BREACHES INVOLVING
500 OR MORE INDIVIDUALS.

SO THEN IT'S
PUBLIC INFORMATION.

SO THAT INFORMATION
WILL BE MADE PUBLIC. YEAH.

>> ARE YOU REFERRING TO--
I KNOW FOR PRIVACY--ON THE

PRIVACY SIDE, WE DO HAVE
LIKE CORRECTIVE ACTIONS

AND IT SHOWS A SECTION THERE
ON WHAT OCR ACHIEVED

IN, UM,
IN OUR INVESTIGATION.

SO I THINK THAT MAYBE--AND
THAT TOOK US A WHILE TO GET

THAT ON THERE. BUT I THINK,
ONCE--LIKE HE SAID,

ONCE--THE BREACH IS NEW,
SO I GUESS

AFTER SEVERAL,
YOU KNOW, INVESTIGATIONS

THEY WILL PROBABLY
DO THE SAME.

BECAUSE I KNOW
FOR PRIVACY WE HAVE IT.

I'M JUST GOING TO SAY

I'M THINKING
THEY'LL [INDISTINCT].

>> OK, WELL, I'LL
CONTINUE TO LOOK.

>> SO YOU MENTIONED
THE BREACH NOTIFICATION

IN THE LAW IS 60 DAYS,
AND WITH PART D

CMS HAS SET A MUCH
SHORTER NOTIFICATION.

WE UNDERSTAND AT ONE POINT
THERE WAS GOING TO BE

DISCUSSIONS BETWEEN OCR AND
CMS WITH REGARDS TO THAT

SO THAT THOSE 2 TIMEFRAMES
COULD BE RECONCILED.

ARE YOU FAMILIAR WITH THAT?

>> NO, I'M NOT.

IF THAT IS TAKING PLACE,

THOSE DISCUSSIONS, THAT'S
WAY ABOVE MY GRADE LEVEL.

AND SO I HAVE TO WAIT
UNTIL IT TRICKLES DOWN.

SO I CAN'T REALLY
ANSWER THAT QUESTION.

>> I DON'T KNOW IF
THIS IS AN EASY QUESTION

OR A HARD ONE.

>> OK.

>> I'LL ASK.

WITH ALL THE CONCERN
ABOUT MAINTAINING PRIVACY

AND PROTECTING HEALTH

INFORMATION, HOW WITH THE

EFFORTS TO INCORPORATE
HEALTH PLANS

INTO WHAT THE CHIP
PROGRAMS ARE DOING

WITH THE UNIQUE I.D.s,

HOW DOES THAT ALL
TIE TOGETHER?

>> WELL, I'M NOT SURE
WHERE YOU'RE GOING

WITH THE UNIQUE I.D.s, BUT IF
THAT'S INDIVIDUALLY IDENTIFIABLE

HEALTH INFORMATION THAT'S
BEING MAINTAINED OR CREATED

BY A COVERED ENTITY
TO HEALTH PLANS,

THEN THAT'S PROTECTED
BY THE PRIVACY RULE.

IF THOSE UNIQUE,
YOU KNOW, UM...

>> THE UNIQUE I.D.s--

THE UNIQUE I.D.s ARE
A CODING, IF YOU WILL,

BETWEEN SHIP COUNSELORS AND
CMS TO ALLOW THE COUNSELORS

TO DISCUSS...
INDIVIDUAL'S ISSUES.

>> OK. WELL, IF THOSE I.D.s--

IF SOMEONE--IF THOSE I.D.s
SOMEHOW HAPPEN TO FALL,

YOU KNOW,
INTO THE PUBLIC DOMAIN,

AND IF SOMEONE COULD
REASONABLY CONNECT

OR RELATE THAT I.D.
TO AN INDIVIDUAL--

YOU CAN DETECT
WHO THE INDIVIDUAL IS,

THEN THAT'S GOING TO BE
A PRIVACY RULE VIOLATION.

IF YOU CAN'T MAKE
THAT ASSOCIATION,

IT'S LIKE THE
IDENTIFIABLE INFORMATION

WHERE YOU JUST TAKE
THESE RANDOM NUMBERS,

AND YOU CAN'T
ASSOCIATE IT WITH ANYONE,

THEN IT WOULDN'T CONSTITUTE
A PRIVACY RULE VIOLATION.

IT WOULD BE CONSIDERED
INDIVIDUAL IDENTIFIABLE HEALTH

INFORMATION BECAUSE YOU CAN'T
ASSOCIATE IT WITH ANYONE.

BUT IF YOU CAN, THEN THAT'S
GOING TO BE CONSTITUTED AS IHI

OR PHI AND THAT WOULD FALL
INTO THE DOMAIN OR WITHIN

THE JURISDICTION
OF THE PRIVACY RULE.

I DON'T KNOW IF THAT
ANSWERS YOUR QUESTION,

IF IT'S GETTING AT--
I'M NOT SURE.

>> [INDISTINCT]

>> OH, OK.

>> ANY MORE QUESTIONS?

ANY MORE QUESTIONS?

ALL RIGHT, WELL--THANK YOU

ALL FOR COMING
TO THE SESSION.

THANK YOU, KELLI ROBINSON
AND ERIC BROWN.

DO YOU HAVE ANY
CLOSING COMMENTS OR--

>> KELLI, YOU SAID SOMETHING YOU
WANTED TO CLARIFY FOR THEM?

>> YOU MADE THE COMMENT
EARLIER WHEN WE FIRST CAME

IN ABOUT THE REPORTING.

WHEN SHE ASKED
ABOUT REPORTING,

AND WAS CMS
AND OCR, UM, CONVERSANT

ABOUT THE TIME PERIOD
FOR REPORTING?

I THINK I WAS UNDER
THE IMPRESSION ALSO

THAT YOU HAD
TO REPORT TO CMS.

BUT THAT HAS
NO BEARING ON OCR.

YOU STILL ARE REQUIRED
TO REPORT WITHIN

A SPECIFIC
TIMEFRAME TO OCR.

>> [INDISTINCT]

>> OK, OK, BECAUSE
HE HAD MENTIONED THAT, TOO.